Analisis Keamanan Protokol Kriptografi SSL/TLS dengan Algoritma ECC pada Layanan Transaksi Online pada *E-Commerce*

Andreana Hartadi Suliman (18220027)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
andreanahs29@gmail.com

***Abstract*— Dalam era digital, keamanan dan integritas data sangat penting dalam komunikasi jaringan. Protokol Secure Sockets Layer (SSL) telah menjadi standar dalam menjaga keamanan dalam layanan transaksi online. SSL menggunakan algoritma kriptografi Elliptic Curve Cryptography (ECC), yang memberikan tingkat keamanan yang tinggi dengan overhead yang lebih rendah dibandingkan dengan algoritma tradisional seperti RSA atau DSA. ECC menggunakan kurva eliptik sebagai dasar perhitungan matematika untuk enkripsi, dekripsi, dan pertukaran kunci yang efisien. Dalam analisis ini, akan dilakukan penilaian terhadap kekuatan enkripsi, keamanan kunci, integritas data melalui tanda tangan digital, dan proteksi terhadap serangan umum terhadap SSL. Tujuan analisis ini adalah memberikan wawasan yang lebih komprehensif tentang keamanan SSL dengan ECC dalam layanan transaksi online. Dengan pemahaman yang lebih baik tentang keamanan SSL dengan ECC, pengembang dan praktisi dapat memilih metode kriptografi yang tepat untuk menjaga keamanan data dalam layanan transaksi online secara efektif dan efisien. Keamanan jaringan dan perlindungan data sensitif merupakan aspek penting yang perlu diperhatikan dalam lingkungan digital yang terus berkembang.**

Keywords—SSL; ECC; Transaksi Online; Kerahasiaan Data; Keamanan Komunikasi Jaringan;

I. PENDAHULUAN

Dalam beberapa tahun terakhir, layanan transaksi online telah mengalami perkembangan pesat dan menjadi pilihan utama bagi banyak individu dan perusahaan. Transaksi keuangan, pembelian barang dan jasa, serta pertukaran informasi sensitif semuanya dilakukan secara daring. Keuntungan yang ditawarkan oleh layanan transaksi online, seperti kenyamanan, kecepatan, dan aksesibilitas global, telah mengubah cara kita berinteraksi dengan dunia digital.

Namun, dengan adanya pertukaran data sensitif dan nilai transaksi yang tinggi, keamanan menjadi faktor yang sangat penting dalam layanan transaksi online. Ancaman terhadap keamanan data, seperti peretasan, pencurian identitas, dan serangan cyber, dapat memiliki konsekuensi yang serius bagi pelanggan dan perusahaan yang terlibat.

Untuk mengatasi risiko ini, perlindungan data yang kuat dan mekanisme keamanan yang andal diperlukan. Protokol kriptografi Secure Sockets Layer (SSL) telah menjadi fondasi keamanan yang umum digunakan dalam layanan transaksi online. SSL memastikan kerahasiaan, integritas, dan autentikasi data yang ditransfer melalui jaringan. Ini dicapai melalui penggunaan teknik enkripsi, tanda tangan digital, serta pertukaran kunci yang aman antara pihak yang terlibat. Dalam konteks keamanan SSL, algoritma Elliptic Curve Cryptography (ECC) telah muncul sebagai solusi yang menjanjikan. ECC menggunakan matematika kurva eliptik untuk melakukan operasi kriptografi.

Algoritma ini menawarkan kekuatan kriptografi yang setara dengan algoritma tradisional, seperti RSA, namun dengan keunggulan efisiensi dan kecilnya ukuran kunci yang dibutuhkan. Hal ini menjadikan ECC sebagai pilihan yang menarik dalam implementasi keamanan SSL pada layanan transaksi online.

Meskipun SSL dengan ECC menawarkan potensi keamanan yang tinggi, pemahaman yang mendalam tentang keamanan dan performa kombinasi ini masih diperlukan. Analisis yang komprehensif tentang penggunaan SSL dengan ECC dalam layanan transaksi online akan memberikan wawasan yang berharga untuk memahami kelebihan, kelemahan, dan tantangan yang dihadapi oleh protokol ini.

Makalah ini bertujuan untuk melakukan analisis mendalam terkait keamanan protokol kriptografi SSL yang menggunakan algoritma ECC dalam konteks layanan transaksi online. Dengan menganalisis aspek-aspek keamanan seperti kerahasiaan data, integritas data, dan autentikasi pengguna, kami akan membahas kekuatan dan kelemahan SSL dengan ECC dalam menghadapi ancaman keamanan yang umum di lingkungan transaksi online.

Melalui analisis ini, diharapkan dapat diperoleh pemahaman yang lebih dalam tentang keamanan protokol SSL yang menggunakan algoritma ECC pada layanan transaksi online. Hasil analisis ini akan memberikan panduan yang berharga bagi pengembang, praktisi, dan peneliti untuk memilih dan menerapkan mekanisme keamanan yang efektif dalam layanan transaksi

II. METODOLOGI PENELITIAN

A. Metode Penelitian

Penelitian ini dilatarbelakangi oleh rasa penasaran penulis terhadap topik yang kemudian didukung oleh studi literatur sebagai validasi. Untuk mengumpulkan data penelitian, penulis melakukan pencarian secara menyeluruh melalui studi literatur yang meliputi sumber-sumber seperti website, jurnal, dan sumber informasi lainnya yang tersedia melalui internet.

B. Batasan Penulisan

Penelitian pada makalah ini dibatasi hanya pada protokol yang digunakan untuk keamanan layanan transaksi online, yaitu pada *e-commerce*.

III. DASAR TEORI

A. Layanan Transaksi Online

Layanan transaksi online mengacu pada proses pembelian, penjualan, atau pertukaran barang, jasa, atau informasi melalui jaringan internet. Ini melibatkan interaksi antara pembeli dan penjual secara elektronik, di mana transaksi dilakukan secara virtual tanpa pertemuan fisik. Contoh layanan transaksi online termasuk e-commerce, perbankan online, pembayaran digital, dan layanan keuangan digital. Layanan transaksi online menawarkan berbagai keuntungan, seperti kenyamanan, aksesibilitas global, fleksibilitas waktu, dan efisiensi. Pengguna dapat mengakses layanan ini kapan saja dan di mana saja, melakukan transaksi dengan cepat, dan menghemat waktu dan tenaga yang diperlukan untuk berpergian ke tempat fisik.

Selain itu, layanan transaksi online sering kali menawarkan berbagai pilihan produk, pembanding harga, dan kemudahan pembayaran. Keamanan merupakan faktor penting dalam layanan transaksi online karena melibatkan pertukaran data sensitif, seperti informasi finansial, detail kartu kredit, dan informasi pribadi. Untuk melindungi keamanan transaksi online, beberapa mekanisme keamanan yang umum digunakan meliputi enkripsi data, autentikasi pengguna, perlindungan terhadap serangan cyber, dan pemantauan aktivitas yang mencurigakan. Layanan transaksi online rentan terhadap berbagai serangan cyber, seperti serangan hacking, serangan DdoS (Distributed Denial of Service), pencurian identitas, serangan phishing, dan serangan malware. Serangan-serangan ini bertujuan untuk mencuri informasi sensitif, mengganggu layanan, atau merusak reputasi bisnis.

Oleh karena itu, perlindungan yang efektif harus diterapkan untuk mencegah dan mengatasi serangan-serangan tersebut. Ada berbagai standar dan protokol keamanan yang digunakan dalam layanan transaksi online untuk memastikan keamanan data dan integritas transaksi. Contohnya adalah Secure Sockets Layer (SSL) dan Transport Layer Security (TLS), yang menyediakan enkripsi data dan autentikasi pihak yang terlibat dalam komunikasi. Selain itu, Payment Card Industry Data Security Standard (PCI DSS) digunakan dalam industri kartu kredit untuk melindungi data kartu kredit.

B. Keamanan Layanan Transaksi Online

Keamanan Layanan Transaksi Online adalah upaya untuk melindungi transaksi yang dilakukan secara elektronik melalui internet atau jaringan komputer. Layanan transaksi online mencakup berbagai jenis transaksi, seperti transaksi keuangan (seperti pembayaran, transfer dana), pembelian produk atau layanan, pendaftaran, dan komunikasi yang melibatkan pertukaran informasi sensitif antara pengguna dan penyedia layanan.

Keamanan dalam layanan transaksi online sangat penting untuk melindungi data sensitif, mencegah penipuan, dan menjaga kepercayaan pengguna terhadap platform atau situs web yang mereka gunakan. Beberapa aspek yang penting dalam keamanan layanan transaksi online meliputi:

- Enkripsi Data: Penggunaan enkripsi data untuk melindungi informasi sensitif saat ditransmisikan melalui jaringan. Enkripsi memastikan bahwa hanya penerima yang dituju yang dapat membaca dan memahami data tersebut.
- Autentikasi: Proses untuk memverifikasi identitas pengguna atau entitas yang terlibat dalam transaksi. Autentikasi dapat melibatkan penggunaan kata sandi, sertifikat digital, atau metode otentikasi lainnya untuk memastikan bahwa pihak yang terlibat adalah pihak yang sah.
- Keamanan Jaringan: Perlindungan terhadap serangan jaringan seperti serangan DDoS, serangan hacking, dan serangan phishing yang dapat mengancam keamanan layanan transaksi online.
- Perlindungan terhadap Malware: Upaya untuk mencegah, mendeteksi, dan menghilangkan malware yang dapat menginfeksi sistem pengguna atau menyebabkan kerugian pada layanan transaksi online.
- Pengelolaan Akses Pengguna: Pengaturan hak akses dan kebijakan keamanan yang ketat untuk memastikan bahwa hanya pengguna yang berwenang yang memiliki akses ke informasi dan fungsi yang relevan.
- Pemantauan dan Deteksi Keamanan: Implementasi sistem pemantauan dan deteksi keamanan yang memungkinkan untuk mendeteksi ancaman keamanan dan mengambil tindakan yang tepat untuk meresponsnya.

Keamanan layanan transaksi online menjadi krusial karena pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data transaksi yang sensitif. Hal ini juga berperan dalam membangun kepercayaan dan kepuasan pengguna terhadap platform atau layanan yang mereka gunakan.

C. SSL (*Secure Sockets Layer)*

Secure Sockets Layer (SSL) adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi jaringan. SSL bekerja pada lapisan transport di atas protokol TCP (*Transmission Control Protocol*) dan digunakan secara luas dalam layanan transaksi online, seperti e-commerce, perbankan online, dan layanan keuangan digital lainnya. SSL menyediakan

kerahasiaan, integritas, dan autentikasi data yang ditransfer antara klien dan server.

Setiap kali pengunjung web mengakses situs yang menggunakan teknologi SSL, situs web akan membentuk sebuah tautan yang terenkripsi antara sesi browser mereka dan web server. SSL merupakan standar industri/protokol untuk komunikasi web yang aman dan digunakan untuk melindungi jutaan transaksi online setiap hari.

SSL memungkinkan informasi sensitif seperti data kartu kredit, nama pengguna, kata sandi, dan informasi penting lainnya ditransmisikan antara server dan klien secara aman karena data yang dikirim akan diacak (dienskripsi).

Sebelum dapat menggunakan koneksi SSL, web server harus memiliki sertifikat SSL. Ketika seseorang mengaktifkan protokol SSL di server web mereka, mereka diminta untuk menjawab pertanyaan yang akan membentuk identitas mereka. Pertanyaan tersebut mencakup informasi tentang situs web dan perusahaan. Setelah sertifikat SSL diterbitkan, server web akan membuat dua kunci kriptografi, yaitu Public Key dan Private Key.

Public Key akan diberikan ke browser bersama dengan sertifikat saat terbentuknya koneksi terenkripsi antara browser dan server. Browser akan menggunakan Public Key ini untuk mengenkripsi data yang akan dikirimkan ke server. Private Key akan digunakan oleh server untuk mendekripsi informasi yang terenkripsi dari browser. Private Key ini sangat rahasia dan tidak boleh diketahui oleh pihak lain karena kunci ini digunakan untuk membuka enkripsi data dari dan ke server. [1]

SSL secara historis telah berkembang menjadi Transport Layer Security (TLS), yang merupakan versi yang lebih baru dan lebih aman dari protokol SSL.

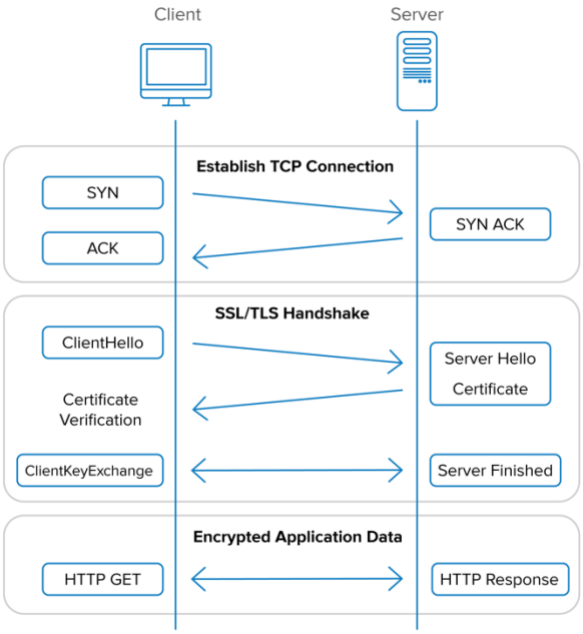
D. TLS

Transport Layer Security (TLS) adalah sebuah protokol keamanan yang digunakan untuk memastikan keamanan komunikasi antara klien dan server melalui jaringan. TLS dirancang dengan tujuan menjaga kerahasiaan, integritas, dan autentikasi data yang dikirimkan melalui jaringan. Dalam konteks keamanan komunikasi web, TLS telah menggantikan protokol sebelumnya yaitu Secure Sockets Layer (SSL) dan telah menjadi standar industri yang umum digunakan.

Pada dasarnya, TLS menggunakan teknik enkripsi untuk melindungi data selama proses transmisi. Dengan menggunakan algoritma enkripsi simetris dan asimetris, TLS memastikan bahwa data yang dikirimkan antara klien dan server hanya dapat dibaca oleh penerima yang dituju. Selain itu, protokol TLS juga memanfaatkan proses Handshake Protocol yang berfungsi untuk melakukan pertukaran informasi antara klien dan server, termasuk negosiasi versi protokol, algoritma enkripsi yang akan digunakan, serta pertukaran kunci publik untuk memastikan keaslian dan integritas komunikasi.

Salah satu komponen penting dalam TLS adalah penggunaan sertifikat digital. Sertifikat digital digunakan untuk memverifikasi identitas server dan klien yang terlibat dalam komunikasi. Sertifikat digital ini dikeluarkan oleh otoritas sertifikat terpercaya dan berisi informasi kunci publik serta tanda tangan digital yang memastikan keaslian sertifikat. Dengan menggunakan sertifikat digital, TLS memastikan bahwa klien dapat mempercayai server yang mereka komunikasikan.

Selain itu, TLS juga melibatkan penggunaan algoritma hash dan message authentication code (MAC) untuk memastikan integritas dan autentikasi data yang ditransmisikan. Fungsi hash digunakan untuk menghasilkan ringkasan data yang diterima, sedangkan MAC digunakan untuk menghasilkan tanda tangan digital yang memverifikasi bahwa data tidak mengalami perubahan oleh pihak yang tidak berwenang.



Gambar 1. Handshake Session

TLS beroperasi pada lapisan transport dalam model referensi TCP/IP, yang memungkinkan penggunaannya di atas berbagai protokol aplikasi seperti HTTP, SMTP, POP, dan lainnya. Dalam konteks layanan transaksi online, penggunaan TLS sangat penting untuk menjaga keamanan dan privasi data sensitif seperti informasi keuangan, identitas pengguna, dan detail transaksi.

Dengan perkembangan teknologi, TLS terus mengalami perbaikan dan peningkatan keamanan. Versi terbaru seperti TLS 1.2 dan TLS 1.3 menawarkan fitur-fitur yang lebih aman dan efisien dalam menjaga keamanan komunikasi. Keseluruhan, TLS berperan penting dalam melindungi komunikasi online dan membangun kepercayaan pengguna terhadap platform atau layanan yang mereka gunakan.

E. Algoritma ECC

ECC (*Elliptic Curve Cryptography*) adalah sebuah algoritma kriptografi yang menggunakan kurva elips sebagai dasar perhitungannya. ECC adalah salah satu metode kriptografi kunci publik yang secara efisien memberikan tingkat keamanan yang

tinggi dengan overhead yang relatif lebih rendah dibandingkan dengan algoritma kriptografi tradisional seperti RSA (Rivest-Shamir-Adleman).

Tabel 1. Perbandingan Algoritma Kunci Publik

Kunci Publik	Masalah Matematis
RSA, Rabin-Williams	Diberikan sebuah bilangan *n*, dicari faktor-faktor primanya
Diffie-Hellman, DSA, ElGamal	Diberikan sebuah bilangan prima *n*, dan bilangan *g* dan *h*, temukan *x* dimana $h = g^x \bmod n$
ECDH, ECDSA	Diberikan sebuah kurva elips *E* dan titik *P* dan *Q* pada *E*, temukan *x* dimana $Q = xP$

Pada dasarnya, ECC menggunakan operasi matematika pada kurva elips untuk melakukan enkripsi, dekripsi, dan pertukaran kunci kriptografi. Algoritma ini mengandalkan kesulitan dalam menyelesaikan persamaan kurva elips diskret (*discrete logarithm problem*) untuk memastikan keamanan data yang dikirimkan. Kurva elips dapat dihitung dengan persamaan matematis berikut:

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

Dalam kriptografi kunci asimetris, ditentukan terlebih dahulu parameter yang akan digunakan dan telah disepakati oleh kedua belah pihak yang akan berkomunikasi. Parameter yang digunakan dalam ECC yaitu nilau *a* dan *b*, bilangan prima *p* dalam persamaan kurva eliptik bidang terbatas serta titik *G* yang dipilih dari kurva eliptik. Pendekatan enkripsi dengan ECC dijelaskan dengan contoh kasus Alice yang akan menerima pesan terenkripsi dari Bob.

- Pembangkitan Kunci Privat dan Kunci Publik
  - Bob membangkitkan kunci privat n_B dengan cara memilih bilangan acak yang nilainya diantara [1, *p*-1]. Dengan kunci privat tersebut, Bob membangkitkan kunci publik $P_B = n_B.G$.
- Enkripsi
  - Misalkan pesan yang dikirim merupakan pesan *m*. Alice akan me-*encode* pesan *m* menjadi sebuah titik P_m dari kurva eliptik. Lalu memilih bilangan acak *k* yang memiliki nilai diantara [1, *p*-1]. Alice akan menghasilkan sebuah cipherteks $C_m = \{(kG), (P_m + kP_B)\}$ dimana *G* adalah titik generator dan P_B adalah kunci public milik Bob.
- Dekripsi
  - Untuk mendekripsi cipherteks C_m, Bob akan mengkalikan titik pertama dari cipherteks dengan kunci privatnya yaitu n_B dan mengurangi titik kedua dari cipherteks dengan hasil perkalian tersebut. Kemudian Bob akan mendecode P_m menjadi pesan *m* semula.

$$P_m + knP_B - n_B(kG) =$$
$$P_m + k(n_BG) - n_B(kG) = P_m \quad (2)$$

Keuntungan dari ECC antara lain adalah kemampuan menghasilkan kunci yang lebih pendek dengan tingkat keamanan yang setara, penggunaan sumber daya komputasi yang lebih efisien, dan kecepatan operasi yang lebih cepat dibandingkan dengan algoritma kriptografi tradisional. Karena itu, ECC sering digunakan dalam aplikasi yang memiliki keterbatasan sumber daya, seperti perangkat mobile, sensor jaringan, dan sistem terdistribusi.

ECC telah digunakan secara luas dalam berbagai protokol keamanan, termasuk protokol SSL untuk keamanan komunikasi web, serta dalam implementasi kriptografi pada sistem keamanan dan aplikasi yang memerlukan tingkat keamanan yang tinggi.

Dalam ECC, terdapat konsep kunci publik dan kunci privat, di mana kunci publik digunakan untuk enkripsi dan verifikasi digital, sedangkan kunci privat digunakan untuk dekripsi dan tanda tangan digital. Kekuatan keamanan ECC didasarkan pada kesulitan dalam memecahkan persamaan kurva elips diskret, yang saat ini dianggap sebagai permasalahan yang sangat sulit untuk dipecahkan secara efisien.

IV. PEMBAHASAN

Protokol SSL/TLS memberikan tiga fungsi keamanan di atas lapisan transport, yaitu kerahasiaan data, integritas data, dan autentikasi. Melalui enkripsi SSL, tiga layanan tersebut dapat memberikan perlindungan terhadap manajemen lalu lintas pada web, seperti konfigurasi, aktivasi, dan penagihan.

Gambar 3. Cara Kerja SSL/TLS pada Aplikasi *E-Commerce* [2]

Selain itu, protokol SSL/TLS juga digunakan secara luas dalam transaksi online, khususnya dalam pembayaran dengan menggunakan kartu kredit melalui internet. Dalam konteks perdagangan elektronik (e-commerce), komunikasi antara pembeli dan penjual dienkripsi untuk menjaga kerahasiaan data yang sensitif, seperti rincian kartu kredit. Selain itu, melalui autentikasi yang dilakukan oleh protokol SSL/TLS, keaslian penjual dapat diverifikasi, sehingga meningkatkan kepercayaan pengguna terhadap transaksi yang dilakukan secara online.

Dengan adanya protokol SSL/TLS, data sensitif yang dikirimkan antara pengguna dan server dapat dilindungi secara efektif dari pihak-pihak yang tidak berwenang. Ini membantu menciptakan lingkungan yang aman dan terpercaya dalam transaksi online, sehingga membangun kepercayaan dan

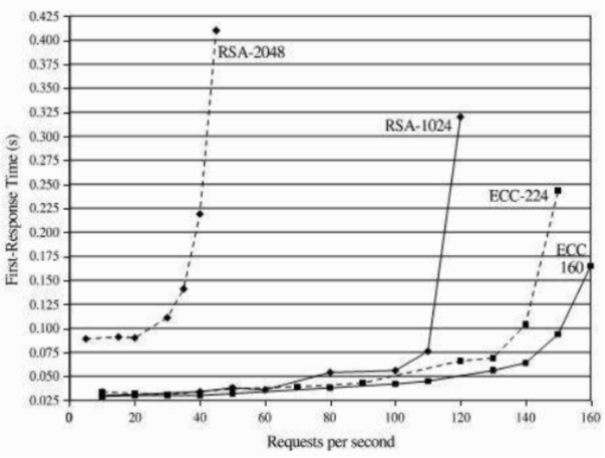
memastikan keamanan bagi pengguna yang berpartisipasi dalam layanan transaksi online.

A. Analisis Keunggulan Algoritma ECC terhadap RSA dalam Penerapan SSL/TLS

Perbandingan antara algoritma Elliptic Curve Cryptography (ECC) dan Rivest-Shamir-Adleman (RSA) dapat diuji melalui percobaan menggunakan beberapa parameter, seperti latensi kriptografi pada tahap handshake, throughput kriptografi server, waktu pembangkitan kunci, dan tingkat keamanan kunci masing-masing. Dalam percobaan ini, empat skenario dilakukan, yaitu RSA dengan panjang kunci 1024, 2048, dan 4096 bit, serta ECC dengan panjang kunci 160, 224, dan 384 bit.

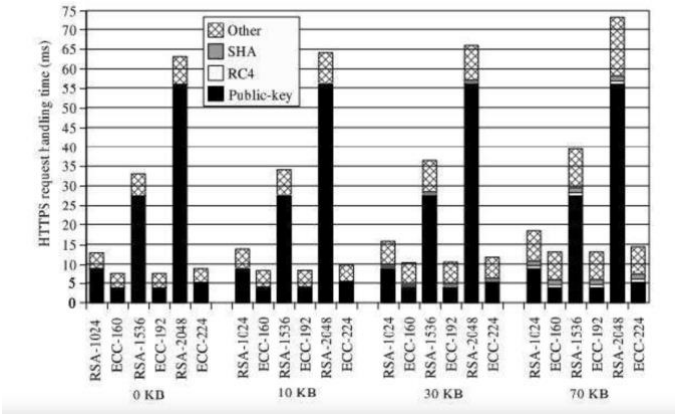
Hasil percobaan menunjukkan bahwa ECC memiliki performa yang lebih baik daripada RSA. ECC memiliki waktu pembangkitan kunci sekitar 73-1300 kali lebih cepat, latensi kriptografi pada tahap handshake yang lebih baik sekitar 1,7 hingga 4 kali (kecuali untuk ECC-160 yang lebih lambat 1,7 kali dibandingkan RSA-1024), dan throughput kriptografi server sekitar 1,5 hingga 16 kali lebih besar (pada otentikasi server saja) dan 2-6 kali lebih besar pada otentikasi penuh (kecuali pada ECC-160 yang lebih kecil 1,5 kali dibandingkan RSA-1024). Selain itu, tingkat keamanan ECC juga lebih tinggi, dengan ketangguhan hingga 103 hingga 1021 kali lebih tinggi daripada RSA.

Grafik yang menunjukkan dampak penggunaan algoritma ECC dan RSA pada waktu respons server juga dapat disimpulkan bahwa untuk menjalankan jumlah lalu lintas web yang sama, penggunaan algoritma RSA memerlukan biaya perawatan server sekitar 3,5 kali lebih besar dibandingkan ECC.



Gambar 4. Perbandingan Latency dan Throughput

Algoritma RSA dan Digital Signature Algorithm (DSA) cenderung memiliki kelemahan dalam hal jumlah bit yang panjang, yang memerlukan waktu perhitungan yang tinggi dan memperlambat pembentukan tanda tangan digital. ECC memiliki keunggulan dibandingkan RSA dan DSA karena menggunakan tanda tangan digital yang lebih pendek dan ukuran kunci yang lebih kecil.



Gambar 5. Perbandingan Waktu Penanganan Request HTTPS pada Server

Ukuran kunci pada Elliptic Curve lebih kecil daripada ukuran kunci pada RSA, namun mampu memberikan tingkat keamanan yang sama. Sebagai contoh, kunci berukuran 160 bit pada Elliptic Curve setara dengan kunci berukuran 1024 bit pada RSA. ECC memiliki kekuatan per bit yang maksimal dibandingkan dengan sistem kriptografi lainnya.

B. *Units*

Alasan penggunaan algoritma Elliptic Curve Cryptography (ECC) dalam transaksi e-commerce dapat dirangkum sebagai berikut:

- ECC mampu menjamin keamanan data yang terlibat dalam transaksi e-commerce.
- ECC menggunakan bandwidth yang lebih efisien dibandingkan dengan alternatif algoritma lain yang digunakan dalam SSL/TLS.
- ECC memungkinkan proses transaksi dilakukan secara lebih efisien, meningkatkan performa keseluruhan transaksi e-commerce.
- Algoritma ECC mengonsumsi daya komputasi dan memori yang lebih rendah dibandingkan dengan algoritma kriptografi lainnya.

Untuk mengimplementasikan ECC dalam TLS, digunakan ECC Cipher Suites. ECC Cipher Suites terdiri dari Elliptic Curve Diffie-Hellman (ECDH) untuk kesepakatan penggunaan kunci pada tahap handshaking TLS, dan Elliptic Curve Digital Signature Algorithm (ECDSA) sebagai mekanisme autentikasi.

KESIMPULAN

Dalam transaksi e-commerce, keamanan data menjadi hal yang penting karena melibatkan data pribadi dan informasi pembayaran yang sensitif. Untuk melindungi data tersebut, diperlukan pengamanan menggunakan kriptografi asimetris, yang melibatkan penggunaan kunci publik dan kunci privat untuk enkripsi dan dekripsi data, serta penggunaan sertifikat untuk memastikan identitas pihak yang terlibat dalam komunikasi.

Secure Sockets Layer (SSL) adalah salah satu solusi yang digunakan untuk mengamankan data dalam transaksi e-commerce. Transport Layer Security (TLS) merupakan pengembangan dari SSL yang lebih baru dan lebih aman.

Algoritma Elliptic Curve Cryptography (ECC) merupakan algoritma yang memiliki tingkat keamanan yang tinggi dengan kunci yang lebih pendek dibandingkan dengan algoritma kriptografi lainnya. Algoritma ECC juga memiliki waktu komputasi yang lebih singkat, sehingga mampu memberikan performa terbaik dalam pengamanan data pada transaksi e-commerce.

PENGHARGAAN

Penulis mengucapkan syukur sebesar-besarnya kepada Tuhan yang Maha Esa karena masih memberikan kesehatan dan atas berkat-Nya sehingga penulis dapat mengerjakan tugas makalah ini. Penulis juga ingin mengucapkan terima kasih atas dukungan teman dan keluarga pada setiap proses pembelajaran.

Penulis ingin mengucapkan syukur juga kepada Bapak Dr. Ir. Rinaldi Munir, M.T. atas bantuannya dan ilmunya yang telah dibagikan pada mata kuliah II4031 Kriptografi dan Koding, yang telah berjasa banyak dalam pengembangan ilmu selama satu semester.

REFERENSI

Berikut adalah referensi yang digunakan untuk pengerjaan makalah ini.

[1] https://sis.binus.ac.id/2019/06/04/pengertian-dan-fungsi-secure-socket-layer-ssl/#:~:text=SSL%20(Secure%20Socket%20Layer)%20adalah,pihak%20lain%20yang%20tidak%20berkepentingan. Diakses pada tanggal 19 Mei 2023.

[2] https://pusatssl.com/cara-kerja-ssl-tls-berkualitas-menjaga-bisnis-online/ diakses pada tanggal 22 Mei 2023.

[3] Sann, Zarni. "Performance Comparison of Asymmetric Cryptography". (2019).

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[5] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 2006.

[6] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

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, 22 Mei 2023

Andreana Hartadi Suliman
18220027