SKRIPSI

IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) DENGAN END-TO-END ENCRYPTION PADA APLIKASI CHAT BERBASIS MOBILE

Disusun dan diajukan oleh:

MUHAMMAD RIDHOI
D121 18 1303

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA
2023

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) DENGAN END-TO-END ENCRYPTION PADA APLIKASI CHAT BERBASIS MOBILE

Disusun dan diajukan oleh

MUHAMMAD RIDHOI
D121181303

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika Fakultas Teknik Universitas HasanuddinPada tanggal 22 Februari 2023 dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

Pembimbing Utama,

Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.
NIP. 19750313 200912 1 003

Pembimbing Pendamping,

Dr. Eng. Muhammad Niswar, S.T., M.IT.
NIP. 19730922 199903 1 001

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu, ST, MT,M.Bus.Sys.,IPM, ASEAN
NIP 19750716 200212 1 004

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama	: Muhammad Ridhoi
NIM	: D121181303
Departemen	: Teknik Informatika
Jenjang	: S1

Menyatakan dengan ini karya tulisan saya berjudul:

"IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DENGAN *END-TO-END ENCRYPTION* PADA APLIKASI *CHAT* BERBASIS *MOBILE*"

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilalihan tulisan orang lain bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 23 Februari 2023

Yang menyatakan,

Muhammad Ridhoi

ABSTRAK

MUHAMMAD RIDHOI. *Implementasi Algoritma Elliptic Curve Cryptography (ECC) Dengan End-To-End Encryption Pada Aplikasi Chat Berbasis Mobile* (dibimbing oleh Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. dan Dr. Eng. Muhammad Niswar, S.T., M.IT.)

Perkembangan aplikasi *mobile* kini sudah tak terkedali. Dapat dilihat dari banyaknya aplikasi yang mampu membantu memenuhi kebutuhan manusia, salah satunya dalam melakukan komunikasi yaitu menggunakan aplikasi *Chatting*. Namun pesan yang dikirim melalui aplikasi *Chatting* sering berisi informasi pesan yang penting bahkan rahasia dan harus dijaga keamanannya dari penyalahgunaan oleh pihak yang tidak berwenang. Salah satu cara yang bisa digunakan untuk menjaga keamanan data ialah kriptografi, dimana terdapat suatu proses data yang dikirim akan disandikan dengan proses enkripsi dan dekripsi. Metode kriptografi yang cocok pada perangkat *mobile* salah satunya adalah *Elliptic Curve Cryptography* (ECC) yang dapat mengurangi biaya komputasi karena metode perkaliannya yang tercepat sehingga menghasilkan pengurangan *overhead* pada proses komputasi. Pada penelitian ini bertujuan untuk membangun aplikasi *chat* berbasis *mobile* yang mengimplementasikan algoritma kriptografi *Elliptic Curve Cryptography* (ECC) untuk mengamankan pesan. Hasil implementasi enkripsi dan dekripsi algoritma *Elliptic Curve Cryptography* (ECC) pada aplikasi *chat* dengan pemantauan *request* yang dikirim ke server, didapati bahwa pesan yang kirim sudah dalam bentuk *ciphertext* sehingga tidak mudah dibaca. Hasil uji kecepatan waktu proses enkripsi dan dekripsi algoritma ECC pada parameter kurva eliptik yang berbeda menunjukkan parameter Secp192r1 28.9% dan 77.1% lebih cepat dibandingkan dengan Secp256r1 dan Secp521r1 pada proses enkripsi, sedangkan pada proses dekripsi 27,9% dan 73.5% lebih cepat dibandingkan Secp256r1 dan Secp521r1. Perbedaan waktu proses enkripsi dan dekripsi dari setiap parameter yang berbeda disebabkan oleh besarnya *overhead* yang ditentukan oleh panjang karakter pesan dan nilai parameter yang digunakan dalam algoritma *Elliptic Curve Cryptography* (ECC).

Kata kunci: Aplikasi *Chat*, Kriptografi, Enkripsi, *Elliptic Curve Cryptography* (ECC)

ABSTRACT

MUHAMMAD RIDHOI. *Implementation of Elliptic Curve Cryptography (ECC) Algorithm with End-To-End Encryption in Mobile-Based Chat Application* (supervised by Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. and Dr. Eng. Muhammad Niswar, S.T., M.IT.)

The development of mobile applications has become unstoppable, as evidenced by the increasing number of applications that help meet human needs, such as communication using Chatting applications. However, messages sent through Chatting applications often contain important or even confidential information that must be kept secure from unauthorized parties. Cryptography is one way to maintain data security, where data sent is encrypted and decrypted. One suitable cryptography method for mobile devices is Elliptic Curve Cryptography (ECC), which can reduce computational costs due to its fast multiplication method, resulting in a reduction in overhead in the computation process. This research aims to develop a mobile-based chat application that implements the Elliptic Curve Cryptography (ECC) algorithm to secure messages. The implementation results of the encryption and decryption algorithms of ECC on the chat application with monitoring of requests sent to the server showed that the sent messages were already in ciphertext form, making it difficult to read. The results of the speed test for the encryption and decryption processes of the ECC algorithm using different elliptic curve parameters showed that the Secp192r1 parameter was 28.9% and 77.1% faster than the Secp256r1 and Secp521r1 parameters for the encryption process, while for the decryption process, it was 27.9% and 73.5% faster than Secp256r1 and Secp521r1. The difference in the encryption and decryption process time for each different parameter is due to the overhead size determined by the length of the message characters and the parameter values used in the Elliptic Curve Cryptography (ECC) algorithm.

Keywords: Chat Application, Cryptography, Encryption, Elliptic Curve Cryptography (ECC)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN DAN ARTI SIMBOL

Lambang/Singkatan	Arti dan Keterangan
a, b	Bilangan konstanta
m	Gradien
mod	Operasi modulus
p	Bilangan prima
x, y	Koordinat titik
P, Q	Titik pada kurva eliptik
k	Skalar, bilangan bulat positif
G	Titik dasar pada kurva eliptik

DAFTAR LAMPIRAN

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala limpahan rahmat dan hidayah yang telah diberikan, sehingga tugas akhir ini bisa diselesaikan. Penulis menyadari bahwa penyelesaian tugas akhir ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih banyak kepada pihak-pihak yang telah banyak memberikan bantuan, dorongan baik moral maupun spiritual. Ucapan terima kasih penulis tujukan kepada:

1. Kedua orang tua penulis, Bapak dan Ibu beserta keluarga atas segala doa, dukungan, semangat, pengorbanan, dan kasih sayang yang telah diberikan.
2. Bapak Dr. Eng. Ady Wahyudi Paundu, ST., M.T. selaku Dosen Pembimbing I yang telah meluangkan waktu dan pikiran dalam memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.
3. Bapak Dr. Eng. Muhammad Niswar, S.T., M.IT. selaku dosen Pembimbing II yang telah meluangkan waktu dan pikiran dalam memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.
4. Seluruh Dosen dan Staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.
5. Para sahabat penulis yang telah memberikan motivasi, nasihat, dukungan, dan semangat selama proses perkuliahan.
6. Teman-teman SYNCHRONOUS selaku rekan belajar sejak awal hingga akhir masa perkuliahan.
7. Seluruh pihak terkait yang tidak dapat penulis sebutkan satu persatu yang telah membantu penulis menyelesaikan penulisan skripsi ini.

Semoga Allah SWT membalas seluruh kebaikan yang telah mereka berikan kepada penulis. Penulis juga menyadari bahwa masih terdapat banyak kekurangan pada penulisan tugas akhir ini. Oleh karena itu, penulis meminta maaf atas segala

kekurangan yang ada pada karya tulis ini. Kritik dan saran sangat penulis harapkan bagi penyempurnaan tugas akhir ini. Semoga tugas akhir ini bisa memberikan manfaat bagi penulis dan pihak lain yang membacanya.

Makassar, Februari 2023

Penulis

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan aplikasi *mobile* kini sudah tak terkedali. Dapat dilihat dari banyaknya aplikasi yang mampu membantu memenuhi kebutuhan dan kepentingan manusia, salah satunya dalam melakukan komunikasi yaitu menggunakan aplikasi *Chatting*. Pengiriman pesan melalui internet dengan menggunakan aplikasi *Chatting* merupakan salah satu metode komunikasi yang bersifat *real-time*. Namun pesan yang dikirim melalui aplikasi *Chatting* sering berisi informasi pesan yang penting bahkan rahasia dan harus dijaga keamanannya dari penyalahgunaan oleh pihak yang tidak berwenang. Aplikasi *Chatting* juga memerlukan sistem keamanan yang baik untuk mengamankan pesan instan bersifat rahasia dan eksklusif. Masalah penyalahgunaan pesan instan pada aplikasi yang berjalan di jaringan internet juga menjadi isu krusial yang harus ditemukan solusinya (Randi dkk., 2020).

Pentingnya menjaga kerahasiaan data yang ada agar mencegah penyalahgunaan pesan yang dikirimkan merupakan salah satu hal yang perlu diperhatikan. Salah satu cara yang bisa digunakan untuk menjaga keamanan data ialah kriptografi. Menurut (Fatonah dkk., 2022) di dalam kriptografi terdapat suatu proses di mana data atau informasi yang dikirimkan akan disandikan (enkripsi dan dekripsi). Enkripsi ini dilakukan saat informasi akan dikirimkan dengan penyandian terlebih dahulu sehingga informasi tersebut akan sulit terbaca. Kemudian proses Dekripsi dilakukan saat penerimaan informasi dengan cara mengubah kembali menjadi bentuk aslinya. Proses Dekripsi hanya bisa dilakukan penerima dengan menggunakan kunci rahasia yang telah disepakati bersama sebelumnya. Kriptografi salah satu cara yang efektif untuk mengatasi ancaman-ancaman terhadap keamanan informasi data, sehingga meskipun data dicuri, informasinya tidak dapat dibaca karena telah disandikan atau dikodekan dengan metode tertentu (Panggabean, 2020). Salah satu metode kriptografi yang dapat mengakomodasi hal tersebut ialah *Elliptic Curve Cryptography* (ECC).

Elliptic Curve Cryptography (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik yang menggunakan kurva eliptik dengan semua variabel dan koefisiennya terbatas pada elemen dari suatu Galois Field. *Elliptic Curve Cryptography* (ECC) juga merupakan teknik kriptografi asimetri yang menggunakan dua buah kunci berbeda dalam proses enkripsi dan dekripsi. Kedua kunci tersebut dikenal dengan *private key* yang digunakan untuk dekripsi data dan *public key* yang digunakan untuk enkripsi data (Damanik, 2019). *Elliptic Curve Cryptography* (ECC) menjadi salah satu pendekatan untuk kemanan siber yang sangat menarik pada perangkat kecil seperti *smartphone*, meteran dan *embedded devices* (Diro dkk., 2017) dengan mekanisme keamanannya dapat mengurangi biaya komputasi, data yang dikirim dan disimpan, karena metode perkaliannya yang tercepat dan memiliki panjang kunci yang pendek (Qazi dkk., 2021).

Elliptic Curve Cryptography (ECC) memiliki kelebihan yaitu memiliki keamanan yang sama dengan algoritma yang lain pada distribusi kunci akan tetapi dengan manajemen kunci lebih baik karena ukuran kunci yang lebih kecil jika dibandingkan dengan algoritma yang lain dan usia dari algoritma ECC ini lebih baru (Pratiwi & Asmunin, 2022). Misalnya, Elliptic Curve Cryptography (ECC) kunci 160 bits setara dengan Rivest Shamir Adleman (RSA) kunci 1024 bits, ECC kunci 224 bits setara dengan RSA kunci 2048 bits. Sehingga *Elliptic Curve Cryptography* (ECC) dapat diterapkan secara luas pada perangkat dengan ruang penyimpanan dan *bandwidth* yang terbatas, karena panjang kunci yang pendek, kecepatan tinggi, dan konsumsi daya yang rendah (Perdana dkk., 2022). Dengan demikian menghasilkan pengurangan *overhead* pada proses komputasi menjadi faktor penting yang membuat ECC menjadi pilihan yang lebih baik dari pada RSA, DSA dan AES (Qazi dkk., 2021).

1.2 Rumusan Masalah

Bagaimana menjaga kerahasiaan dan keamanan pesan teks dari penyalahgunaan oleh pihak yang tidak berwenang dengan *Elliptic Curve Cryptography* (ECC) secara *End-to-End* pada aplikasi *Chat* berbasis *Mobile*?

1.3 Tujuan Penelitian

1. Mengimplementasikan sistem kriptografi algoritma *Elliptic Curve Cryptography* (ECC) pada aplikasi *Chat* berbasis *Mobile* dalam menjaga kerahasiaan dan keamanan pesan teks secara *End-to-End* dari penyalahgunaan oleh pihak yang tidak berwenang.
2. Menganalisa parameter standar kriptografi kurva eliptik Secp192r1, Secp256r1, dan Secp521r1 pada enkripsi dan dekripsi algoritma *Elliptic Curve Cryptography* (ECC).

1.4 Manfaat Penelitian

1. Membantu masyarakat dalam menjaga kerahasiaan dan keamanan pesan teks yang dikirim maupun diterima tetap aman.
2. Mengetahui sejauh mana peran *Elliptic Curve Cryptography (ECC)* dalam menjaga kerahasiaan dan keamanan pesan teks.
3. Menjadi dasar untuk penelitian terkait sistem kripto dengan *Elliptic Curve Cryptography (ECC)*.

1.5 Ruang Lingkup

1. Pengembangan aplikasi *Chat* menggunakan *framework* Flutter berbasis Android.
2. Menggunakan bahasa pemrograman Dart.
3. Karakter pada pesan teks yang di enkripsi ialah ASCII.
4. Informasi yang dienkripsi dan didekripsi berupa pesan teks.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini akan dijelaskan teori-teori yang menunjang percobaan yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi analisis kebutuhan sistem, perancangan implementasi sistem, implementasi algoritma, skenario penggunaan dan skenario pengujian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi hasil penelitian dan pembahasan.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil penelitian dan saran

BAB II
TINJAUAN PUSTAKA

2.1 Kriptografi

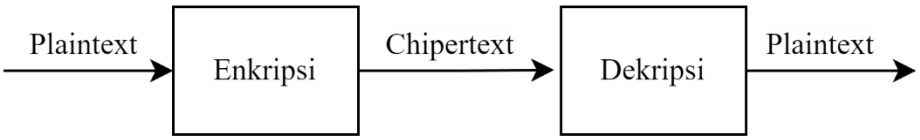
Kriptografi berasal dari gabungan dua kata yaitu “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan. Dalam bahasa komputasi kriptografi diartikan sebagai ilmu dan seni untuk menjaga keamanan data. Ahli kriptografi disebut kriptografer. Kriptografi merupakan salah satu cara untuk mencegah kebocoran data yang bersifat rahasia, dimana dalam memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut (Amrulloh & Ujianto, 2019).

Beberapa istilah yang digunakan dalam bidang kriptografi yaitu:

1. *Plaintext* adalah pesan asli yang hendak dikirimkan (berisi data asli) berupa kumpulan karakter yang dapat berupa abjad, angka atau simbol tertentu yang dapat dibaca.
2. *Chiphertext* adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi dari algoritma enkripsi yang tidak dapat dibaca secara langsung.
3. Enkripsi, salah satu proses utama dalam kriptografi dimana suatu proses di mana sebuah pesan asli (*plaintext*) diubah menjadi bentuk pesan lain yang tidak dapat dibaca (*ciphertext*) menggunakan suatu fungsi matematis kunci tertentu yang disebut key, dalam upaya pengamanan data yang dikirimkan terjaga rahasianya.
4. Dekripsi, merupakan kebalikan dari enkripsi, dimana ciphertext dirubah kembali ke plaintext dengan menggunakan fungsi matematis dan key, atau proses pesan yang telah dienkripsi dikembalikan seperti semula.

5. Kunci, atau *key* digunakan dalam proses melakukan enkripsi dan dekripsi. *Key* terbagi menjadi dua bagian yaitu kunci privat dan kunci umum atau kunci publik.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Enkripsi adalah suatu proses yang melakukan perubahan dari suatu pesan yang bisa dibaca menjadi tidak dapat dibaca. Dekripsi adalah suatu proses untuk mengembalikan informasi yang tidak bisa dimengerti tadi menjadi seperti semula (Amrulloh & Ujianto, 2019). Proses enkripsi dan dekripsi kriptografi dapat dilihat pada gambar 1.



Gambar 1 Proses Ekripsi dan Dekripsi

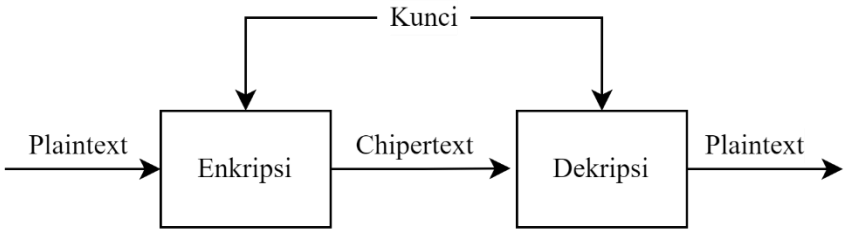
Secara umum ada dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern, Kriptografi klasik (simetris) adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa dilakukan adalah substitusi dan transposisi. Sedangkan kriptografi modern (asimetrik) adalah algoritma yang lebih kompleks dari pada algoritma klasik, hal ini disebabkan algoritma ini menggunakan komputer (Sumandri, 2017).

2.1.1 Kriptografi Simetris

Kriptografi simetri atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi (Sumandri, 2017). Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Dalam kriptografi simetri, kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Keamanan dari pesan yang menggunakan kriptografi simetri ini tergantung pada kuncinya, jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut. Jadi pembuat

pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut, termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia *ciphertext* (Basri, 2016)

Secara sederhana proses enkripsi dan dekripsi dengan kriptografi simetri dapat digambarkan pada gambar 2.



Gambar 2 Skema Kriptografi Simetri

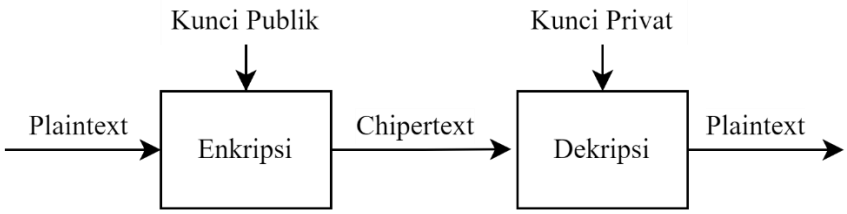
2.1.2 Kriptografi Asimetris

Kriptografi Asimetris atau biasa juga disebut dengan algoritma kriptografi kunci publik yaitu kriptografi yang menggunakan dua buah kunci yang berbeda dalam proses enkripsi dan deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci private untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya (Basri, 2016).

Gambaran umum kriptografi asimetris dapat dilihat pada gambar 3.

Pada kriptografi asimetris, kuncinya terbagi menjadi dua bagian yaitu:

1. Kunci publik (*public key*) yaitu kunci yang dapat mengenkripsi data dan boleh didistribusikan secara luas tanpa memengaruhi keamanan.
2. Kunci privat (*private key*) yaitu kunci yang dirahasiakan atau hanya pemakai yang mempunyai akses kunci dapat mengdekripsi data enkripsi tersebut.

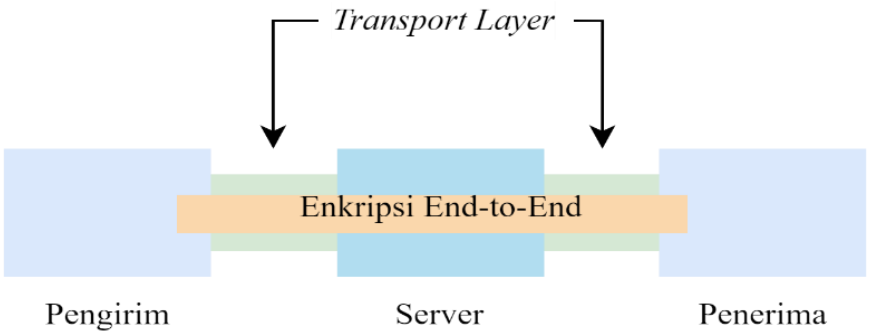


Gambar 3 Skema Kriptografi Asimetris

2.1.3 Sistem Enkripsi *End-to-End*

Enkripsi *end-to-end (End-to-end Encryption)* adalah salah satu yang paling banyak digunakan untuk pengamanan pengiriman informasi melalui internet. Pada dasarnya, enkripsi *end-to-end* merupakan jenis enkripsi dalam suatu sistem komunikasi yang dilakukan terhadap pesan sebelum dikirim oleh pengirim dan kembali didekripsi saat pesan sampai ke penerima, dalam artian enkripsi data dilakukan pada sumber pengiriman pesan dan kemudian didekripsi hanya pada tujuan akhir atau penerima pesan. Dengan enkripsi *end-to-end*, informasi dapat dikirim melalui jaringan dengan satu jalur yang hanya pengirim dan penerima yang bisa mengaksesnya sehingga informasi yang dikirim dari pengirim pesan dikemas dalam bentuk kunci khusus yang hanya bisa dideskripsikan oleh penerima (Santria & Arsoetar, 2017).

Adapun ilustrasi dari enkripsi *end-to-end* dapat dilihat pada gambar 4.



Gambar 4 Ilustrasi Enkripsi *End-to-End*

2.2 Algoritma *Elliptic Curve Cryptography*

Elliptic Curve Cryptography atau Kriptografi Kurva Eliptik adalah sebuah algoritma kriptografi kunci publik, yaitu algoritma dimana setiap pihaknya memiliki sepasang kunci privat dan kunci publik. Kunci privat hanya dimiliki oleh pribadi-pribadi yang berkepentingan, sedangkan kunci publik disebarluaskan ke semua pihak (Santoso & Siambaton, 2020). *Elliptic Curve Cryptography* menjadi salah satu pendekatan kriptografi kunci asimetris yang mendasarkan keamanannya pada persoalan logaritma diskrit dari kurva eliptik bidang terbatas. Struktur kurva eliptik digunakan sebagai grup operasi matematis untuk melangsungkan proses enkripsi dan dekripsi. Salah satu kegunaan ECC yaitu skema enkripsi yang menggunakan algoritma ECC ElGamal (Nugroho & Munir, 2015).

Kurva ellips dalam kriptografi dicetuskan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Kurva ellips juga digunakan pada beberapa algoritma pemfaktoran integer yang juga memiliki aplikasinya dalam kriptografi, seperti *Lenstra Elliptic Curve Factorization*. Algoritma kunci publik ini, berdasarkan pada variasi perhitungan matematis yang terbilang sangat sulit dipecahkan tanpa pengetahuan tertentu mengenai bagaimana perhitungan tersebut dibuat (Mardianto dkk., 2015). Pendekatan yang dilakukan untuk menghasilkan algoritma Kriptografi Kurva Eliptik adalah dengan menggunakan struktur matematika yang sangat unik yang memungkinkan pemrosesan titik dengan memiliki dua buah titik dalam sebuah kurva eliptik dan menghasilkan sebuah titik lain yang ada pada kurva tersebut. Struktur yang unik ini memberikan keuntungan dalam kriptografi dikarenakan kesulitan untuk menemukan 2 buah titik yang menentukan sebuah titik tertentu tersebut tidak dapat ditemukan dengan mudah. Tingkat kesulitan untuk menemukan 2 buah titik termasuk dalam golongan yang rumit sama seperti kesulitan untuk memperhitungkan 4 variasi eksponensial yang digunakan dalam algoritma RSA yang telah banyak diimplementasikan. Untuk memecahkan Kriptografi Kurva Eliptik sendiri dibutuhkan perhitungan matematis yang sangat tinggi (Santoso & Siambaton, 2020).

Elliptic Curve Cryptography (ECC) mempunyai keuntungan jika dibandingkan dengan kriptografi asimetris lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Sebagai perbandingan, 160 bit *Elliptic Curve Cryptography* mempunyai tingkat keamanan (3.8.1010 MIPS/*Million Instruction per Second year*) yang sama dengan 1024 bit RSA mempunyai tingkat keamanan (3.1012 MIPS year). Sehingga kecepatannya lebih tinggi, konsumsi daya yang lebih rendah, adanya penghematan *bandwith* (Br Sembiring, 2015).

Kumpulan titik pada kurva dapat membentuk kumpulan abelian (dengan titik pada tak terhingga sebagai elemen identitas). Jika nilai x dan y dipilih dari daerah finite yang besar, solusi akan membentuk suatu kumpulan abelian finite. Permasalahan logaritma diskrit pada kumpulan kurva ellips tersebut dipercaya lebih sulit dibandingkan permasalahan yang sama (perkalian bilangan tidak nol) dalam daerah finite. Sebagai salah satu kriptosistem kunci publik, belum ada pembuktian matematis untuk tingkat kesulitan dari ECC yang telah dipublikasikan sampai tahun 2006. Tetapi U.S. National Security Agency telah mengesahkan teknologi ECC sebagai algoritma kriptografi yang dianjurkan (Mardianto dkk., 2015)

Medan berhingga atau biasa disebut juga sebagai *Galois Field* (GF) yaitu medan himpunan bilangan yang memiliki bilangan yang terbatas. *Order* dari medan berhingga yaitu jumlah banyaknya elemen yang ada dalam medan tersebut. Medan berhingga dilambangkan sebagai GF(q), dimana q adalah derajat medan berhingga yang berupa pangkat prima. Dalam merepresentasikan elemen Fq dengan $q = p^m$ maka p disebut sebagai karakteristik dari Fq dan m disebut sebagai derajat perluasan dari Fq, dimana p adalah bilangan prima dan m adalah bilangan bulat positif. Medan berhingga yang digunakan dalam *Elliptic Curve Cryptography* adalah Fq dengan $q = p$ dan $q = 2^m$ dengan $q = p$ disebut bidang prima dan dinotasikan sebagai Fp.

2.2.1 Operasi Matematika *Elliptic Curve Cryptography*

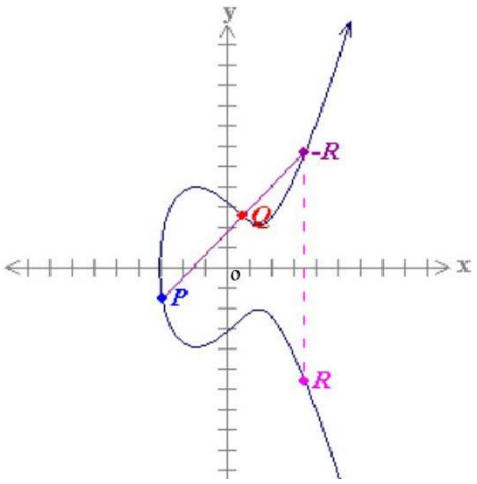
Persamaan matematika dari kurva eliptik pada bidang prima Fp yang digunakan pada *Elliptic Curve Cryptography* adalah sebagai berikut:

$x^3 + ax + b \; mod \; p$, dimana $4a^3 + 27b^2 \; mod \; p \; \neq \; 0$ (1)

Pada elemen bidang berhingga menggunakan bilangan bulat antara 0 dan p – 1. Aritmatika modular pada semua operasi seperti penambahan, pengurangan, pembagian, dan perkalian melibatkan bilangan bulat antara 0 dan p – 1. Bilangan prima p ditentukan dengan nilai tertentu, sehingga ada sebagian besar titik pada kurva eliptik memberikan sistem kriptografi yang aman. *Elliptic Curve Cryptography* memiliki tiga operasi utama yaitu penjumlahan titik, penggandaan titik, dan perkalian titik (Boruah & Saikia, 2014).

2.2.1.1 Penjumlahan Titik

Penjumlahan titik adalah penambahan dua titik berbeda yang menghasilkan koordinat titik ketiga. Koordiant titik ketika dihasilkan dari titik pada kurva eliptik yang dilalui garis yang ditarik dari koordinat dua titik tersebut dan diinvers terhadap sumbu x, sehingga sumbu y negatif dari y titik tersebut. Penjumlahan dua titik pada kurva eliptik dapat dilihat pada gambar 5.



Gambar 5 Penjumlahan dua titik pada kurva eliptik

Dua titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$ adalah titik terpisah. $P + Q = R(x_3, y_3)$, dicari dengan perhitungan:

$$x_3 = m^2 - x_1 - x_2 \; mod \; p \qquad (2)$$

$$y_3 = m(x_1 - x_3) - y_1 \; mod \; p \qquad (3)$$

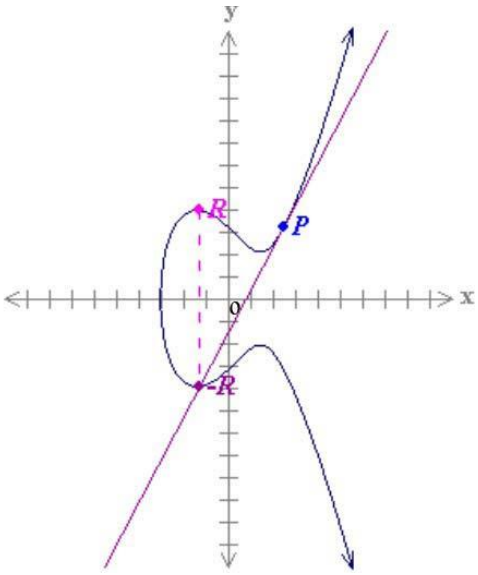
Dimana gradien (m):

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad (4)$$

Dimana (x_1, y_1) koordinat titik pertama, (x_2, y_2) titik kedua dan (x_3, y_3) titik ketiga hasil perhitungan (Boruah & Saikia, 2014).

2.2.1.2 Penggandaan Titik

Penggandaan titik merupakan penjumlahan titik yang dijumlahkan dengan dirinya sendiri atau pada koordinat yang sama. Penggandaan titik membentuk tangen pada titik $P(x_1, y_1)$. Penggandaan titik pada kurva eliptik dapat dilihat pada gambar 6.



Gambar 6 Pengandaan Titik pada Kurva Eliptik

Penggandaan titik $P(x_1, y_1)$ dalam kurva eliptik, garis singgung ke kurva harus melintasi kurva melalui titik lain, ditulis sebagai $-R$ kemudian merefleksikan titik $-R$ pada sumbu x ke titik R dimana $R = 2P$ dengan $R = (x_2, y_2)$, maka:

$$x_2 = m^2 - 2x_1 \; mod \; p \qquad (5)$$

$$y_2 = m(x_1 - x_3) - y_1 \; mod \; p \qquad (6)$$

Dimana gradien (m):

$$m = \frac{3{x_1}^2 + a}{2y_1} \qquad (7)$$

Dimana (x_1, y_1) koordinat titik asal dan (x_2, y_2) koordinat hasil perhitungan (Boruah & Saikia, 2014).

2.2.1.3 Perkalian Titik

Perkalian titik skalar merupakan blok dari semua kriptosistem kurva eliptik dengan Operasi dari bentuk kP, dimana P adalah titik pada kurva eliptik dan k adalah bilangan bulat positif. Menghitung kP berarti menambahkan titik P tepat $k - 1$ kali untuk diriya sendiri, yang menghasilkan titik lain Q pada kurva eliptik.

Perkalian titik menggunakan dua operasi dasar kurva eliptik diantaranya penjumlahan titik dan pengandaan titik. Misalnya menghitung $kP = Q$, jika $kP = 23P$ maka $kP = 23P = 2(2(2(2P) + P) + P) + P$, jadi untuk mendapatkan hasilnya, penjumlahan titik dan perkalian titik akan digunakan secara berulangkali (Boruah & Saikia, 2014).

2.2.2 Enkripsi dan Dekripsi Algoritma *Elliptic Curve Cryptography*

Dalam persoalan logaritma diskrit dari kurva eliptik, diberikan P dan Q yang merupakan dua buah titik di kurva eliptik, carilah integer k sedemikian sehingga Q = kP. Secara komputasi sulit untuk menemukan k, jika k adalah bilangan yang besar. Bilangan k merupakan logaritma diskrit dari Q dengan basis P. Pada ECC, Q adalah kunci publik, k adalah kunci privat, dan P adalah sembarang titik pada kurva eliptik.

Dalam kriptografi kunci asimetris, harus ditentukan terlebih dahulu nilai parameter yang akan digunakan dan telah disepakati oleh pihak yang akan berkomunikasi. Parameter yang digunakan dalam ECC yaitu nilai a dan b, bilangan prima p dalam persamaan kurva eliptik bidang terbatas serta titik generator G yang dipilih dari kurva eliptik. Pendekatan enkripsi dan dekripsi dengan ECC ini dapat dijelaskan dalam contoh kasus misalnya Alice ingin mengirim pesan yang terenkripsi kepada Bob berikut ini (Nugroho & Munir, 2015) :

1. 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 $P_B = n_B \, . \, G$.

2. Enkripsi

   Misalnya pesan yang akan dikirim adalah pesan m. Alice meng-encode pesan m menjadi integer nilai ASCII. Lalu memilih bilangan acak k yang nilai diantara $[1, p-1]$, kemudian dinyatakan x = (m.k) + 1, lalu sulihkan x kedalam persamaan kurva eliptik hingga mendapatkan nilai y, sehingga didapatkan pesan (Pm) telah menjadi

titik (x,y). Terakhir, Alice menghasilkan cipherteks (*Cm)*, yang terdiri dari pasangan titik $Cm = \{(kG), (Pm + kPB)\}$ dimana G adalah titik generator dan P_B adalah kunci publik Bob.

3. Dekripsi

   Untuk melakukan dekripsi cipherteks *Cm*, Bob mula-mula mengalikan titik pertama dari cipherteks dengan kunci privatnya n_B dan kemudian mengurangkan titik kedua dari cipherteks dengan hasil perkalian tersebut.

   $$Pm + kPB\ nB(kG) = Pm + k(nBG)\ nB(kG) = Pm$$

   Terakhir decode Pm (m = (x-1/n)) menjadi pesan m semula.

2.3 Chatting

Chatting ialah kegiatan berkomunikasi dalam dunia internet atau suatu fiture dalam internet untuk berkomunikasi langsung sesama pemakai internet yang sedang online. Anda dapat mengirimkan pesan kepada orang lain yang sedang online kemudian orang yang dituju akan merespon dengan membalas pesan Anda, demikian seterusnya. *Chatting* menggunakan metode komunikasi dua arah dimana data yang ditransmisikan atau dikirim dapat dilakukan secara dua arah dan dapat saling mengirimkan data secara bersama-sama. Bentuk komunikasi saat *chatting* dapat berupa suara, teks atau dalam bentuk video langsung dan berbicara tanpa teks. *Chatting* dapat terjadi di dalam percakapan umum maupun langsung melalui pesan pribadi. Pada dasarnya proses *chatting* membutuhkan sebuah aplikasi yang memfasilitasi terjadinya komunikasi *chatting*, dimana saat ini telah banyak aplikasi-aplikasi *chatting* yang bermunculan sesuai dengan kelebihan dan kekurangan masing-masing yang telah memberikan fasilitas pelayanan kepada setiap penggunanya (Fahlevie, 2012).

2.4 Aplikasi *Mobile*

Aplikasi *Mobile* adalah proses dimana pengembangan aplikasi untuk perangkat genggam seperti telepon genggam atau PDA. Dengan menggunakan aplikasi mobile dapat mempermudah berbagai macam aktivitas seperti hiburan,

maupun pekerjaan (Priyantono, 2019). Melalui aplikasi mobile, pengguna juga dapat mengakses sejumlah informasi informasi penting menggunakan smartphone yang terkoneksi dengan layanan internet. Perangkat mobile memiliki banyak jenis dalam ukuran desain dan tampilan namun memiliki karakteristik yang berbeda dengan desktop system. Selain itu perangkat mobile juga memiliki ukuran yang kecil serta memori yang terbatas. Selama manufaktur aplikasi mobile sudah ada atau bisa didownload oleh pemakai sesuai dengan platform perangkat lunaknya (Adha Bilqis Ibrahim & Gustina, 2021). Secara umum, aplikasi mobile memungkinkan penggunanya terhubung ke layanan internet yang biasanya hanya diakses melaului PC atau Notebook. Dengan demikian, aplikasi mobile dapat membantu pengguna untuk lebih mudah mengakses layanan internet menggunakan perangkat mobile mereka (Kadi, 2017).

2.5 Android

Android adalah sebuah sistem operasi pada handphone yang berbasis pada sistem operasi Linux dan bersifat terbuka sehingga sebuah aplikasi dapat memanggil salah satu fungsi inti ponsel seperti membuat panggilan, mengirim pesan teks, menggunakan kamera dan lain-lain. Android bisa digunakan oleh setiap orang yang ingin menggunakannya pada perangkat mereka. Salah satu keunggulan Android yaitu sebuah mesin virtual yang dirancang khusus untuk mengoptimalkan sumber daya memori dan perangkat keras yang terdapat di dalam perangkat dan menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri yang akan digunakan untuk bermacam peranti bergerak. Android menyediakan akses yang sangat luas kepada pengguna untuk menggunakan aplikasi yang semakin baik. Android memiliki sekumpulan *tools* yang dapat digunakan sehingga membantu para pengembang dalam meningkatkan produktivitas pada saat membangun aplikasi yang dibuat (Priyantono, 2019).

2.6 Flutter

Menurut (Adha Bilqis Ibrahim & Gustina, 2021) Flutter adalah kerangka antarmuka pengguna portabel (UI) Google untuk membangun aplikasi modern, asli, dan reaktif untuk berbagai platform. Flutter menggunakan *widget* untuk membuat UI. Flutter menggunakan mesin rendernya sendiri untuk menggambar *widget*. Elemen memiliki referensi ke *widget* dan bertanggung jawab untuk membandingkan perbedaan *widget*. Selain itu Flutter juga salah satu Software Development Kit (SDK) buatan Google yang berfungsi untuk membuat aplikasi mobile, baik untuk Android maupun iOS .Dengan Flutter, aplikasi Android dan iOS dapat dibuat menggunakan basis kode dan Bahasa pemrogaman yang sama yaitu Dart, bahasa pemrograman yang juga diproduksi oleh Google pada tahun 2011 (Luthfi, 2020). Salah satu keunggulan Flutter ialah semua kodenya di *compile* dalam kode *native* nya (Android NDK, LLVM, AOT-compiled) tanpa ada intrepeter pada prosesnya sehingga proses *compile*-nya menjadi lebih cepat.

2.7 Dart

Dart adalah sebuah bahasa pemrograman yang dikembangkan oleh Google, dirancang oleh Lars Bak dan Kasper Lund. Dart pertama kali dikenalkan pada 10 Oktober 2011 (Luthfi, 2020). Bahasa pemrograman ini dikembangkan sebagai bahasa pemrograman aplikasi yang dapat dengan mudah untuk dipelajari dan juga merupakan bahasa pemrograman berbasis *class* dan berorientasi terhadap obyek dengan menggunakan sitaks bahasa pemrograman. Dart dapat digunakan untuk membuat aplikasi server (berbentuk *commandline interface*), web, desktop, maupun mobile (Android dan iOS). Bahasa pemrograman Dart dapat digunakan secara bebas oleh para developer, karena bahasa ini dirilis secara *open-source* oleh Google di bawah lisensi BSD (Adha Bilqis Ibrahim & Gustina, 2021).

2.8 Firebase

Firebase adalah *Cloud Service Provider* dan *Backend as a Service* yang dimiliki oleh google. Firebase merupakan solusi yang ditawarkan oleh Google

untuk mempermudah dalam pengembangan aplikasi mobile maupun web. Firebase memiliki produk utama, yaitu menyediakan *backend* sebagai layanan *(Backend as a Service)* dan *database* realtime yang membuat data tetap terhubung di aplikasi klien melalui *listener realtime* dan menawarkan dukungan secara *offline* untuk seluler dan web sehingga dengan begitu dapat dibuat aplikasi yang responsif dan mampu bekerja tanpa harus bergantung pada latensi jaringan atau koneksi Internet. Layanan ini menyediakan pengembang aplikasi API yang memungkinkan aplikasi data yang akan disinkronisasi di klien dan disimpan di *cloud* Firebase ini (Adha Bilqis Ibrahim & Gustina, 2021).

2.9 Android Studio (IDE)

Menurut (Adha Bilqis Ibrahim & Gustina, 2021) Android Studio merupakan Integrated Development Enviroment (IDE) untuk system operasi Android, yang dibangung diatas perangkat lunak JetBrains IntelliJ IDEA dan didesain khusus untuk pengembangan aplikasi Android. IDE ini pertama kali diperkenalkan oleh Google dan diumumkan pada Mei 2013. Android studio memiliki beberapa keungulan diantaranya :

1. Editor kode yang cerdas, android studio membantu untuk membuat kode dengan cepat, dengan fitur intelligent code editor yang memberikan kemudahan dalam menganalisis kode dan menyediakan saran kode yang akan digunakan dengan sistem auto complete.
2. Android studio menyediakan layout editor yang lebih bagus dan Bisa melakukan build pada beberapa APK.
3. Dioptimalkan untuk seluruh perangkat android
4. Firebase assistant membantu menghubungkan aplikasi dengan Firebase dan menambahkan layanan seperti Analytics, Autentikasi, Notifikasi, dan lainnya dengan prosedur sesuai dengan urutan di dalam Android Studio.

2.10 Penelitian Terkait

Berikut ini adalah beberapa penelitian terdahulu yang berkaitan dengan penelitian yang akan dilakukan :

Pada tahun 2021 penelitian oleh Danang H. Sulaksono, Citra N. Prabiantissa, Gusti E. Yuliastuti dan Ainur R. Taqwadari dari Jurusan Teknik Informatika, Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya pada jurnal penelitian yang berjudul Implementasi Kriptografi dengan Metode *Elliptic Curve Cryptography* (ECC) untuk Aplikasi *Chatting* Berbasis Android. Penelitian ini membahas proses enkripsi (penyandian data) dan proses dekripsi (pengembalian data asli) pesan dengan algoritma *Elliptic Curve Cryptography* (ECC) pada aplikasi *chatting*. Parameter yang digunakan dalam mengukur efektivitas dari metode Algoritma *Elliptic Curve Cryptography* (ECC) yaitu *Avalanche Effect* yang akan menunjukkan bahwa suatu metode cocok digunakan untuk menyelesaikan masalah yang sedang terjadi saat ini. Hasil pengujian menunjukkan bahwa algoritma *Elliptic Curve Cryptography* (ECC) efektif untuk menyembunyikan *file* data pada aplikasi *chatting* yang bersifat privasi dengan hasil percobaan sebanyak 25 data citra didapatkan nilai *Avalanche Effect* terkecil adalah 26.528016 dan nilai *Avalanche Effect* terbesar adalah 94.67749 dengan rata – rata sebesar 79.88819. Hasil persentase yang cukup besar membuktikan bahwa aplikasi berjalan dengan baik, karena semakin besar nilai persentase yang didapat maka semakin baik aplikasi itu berjalan.

Pada tahun 2022 penelitian oleh Julieta Adhellia Pratiwi dan Asmunin dari Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya pada jurnal penelitian yang berjudul Penggunaan QR *code* Berbasis Kriptografi Menggunakan Algoritma *Elliptic Curve Criptography (ECC)*. Penelitian ini membahas proses enkripsi (penyandian data) dan proses dekripsi (pengembalian data asli) URL dengan algoritma *Elliptic Curve Cryptography* (ECC) pada QR Code. Kinerja yang diukur dari algoritma *Elliptic Curve Criptography (ECC)* ini, waktu komputasi yang dibutuhkan dalam melakukan enkripsi dan dekripsi data. Sebuah QR Code dengan implementasi algoritma *Elliptic Curve Criptography (ECC)* ini. Hasil Pengujian penerapan algoritma ECC digunakan untuk enkripsi dan dekripsi URL beberapa data penting dengan kecepatan dan performa *Elliptic Curve Criptography* diperoleh hasil rentan waktu rata-rata 0.00895 detik pada proses enkripsi dan waktu rata-rata

0.015878 detik pada proses dekripsi, menunjukkan semakin panjang masukkan diperoleh semakin banyak jumlah karakter semakin lama proses enkripsi dan dekripsi yang dibutuhkan.

Pada tahun 2021 penelitian oleh Ummu Wachidatul Latifah dan Puguh Wahyu Prasetyo dari Departemen Matematika, Fakultas Sains dan Teknologi Terapan dan Departemen Pendidikan Matematika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Ahmad Dahlan Yogyakarta pada jurnal penelitian yang berjudul Implementasi Kriptografi Kurva Eliptik Elgamal di Lapangan Galois Prima pada Proses Enkripsi dan Dekripsi Berbantuan *Software* Python. Penelitian ini membahas proses pembentukan kunci kurva eliptik, enkripsi (penyandian data) dan proses dekripsi (pengembalian data asli) dengan mengimplementasikan algoritma Kriptografi Kurva Eliptik Elgamal di Galois Field prima dengan menggunakan *software* Python. Hasil implementasi Kriptografi Kurva Eliptik ElGamal pada Galois Field prima menghasilkan sistem yang aman untuk menjaga kerahasiaan sebuah pesan dengan perhitungan titik – titik kurva eliptik yang rumit, sehingga hal tersebut sangat sulit diretas keamanannya. Hasil pembentukan kunci diperoleh kunci publik dan kunci privat. Input dari proses enkripsi berupa plaintext yang dienkripsi menggunakan kunci publik dan pada proses dekripsi memiliki input berupa ciphertext dan kunci privat dengan output berupa cipher text.

Pada tahun 2019 penelitian oleh Putri S E A Damanik dari jurusan Teknik Informatika, STMIK Budi Darma pada jurnal penelitian yang berjudul Implementasi Algoritma *Elliptic Curve Cryptography* (ECC) Untuk Penyandian Pesan Pada Aplikasi *Chatting Client Server* Berbasis Desktop. Penelitian ini membahas proses pembentukan kunci dan proses enkripsi (penyandian data) pesan teks dengan algoritma *Elliptic Curve Cryptography* (ECC) pada aplikasi *chatting client server* berbasis dekstop. Sebuah aplikasi yang dapat meng-enkripsi dan dekripsi sebuah pesan teks dengan implementasi algoritma *Elliptic Curve Criptography (ECC)*. Didapatkan hasil dengan konsep pengiriman pesan berdasarkan jaringan *peer to peer* dimana *client* dan *server* terhubung dalam jaringan untuk dapat melakukan pengiriman pesan dengan penerapan algoritma *Elliptic Curve Criptography (ECC)* dapat mengamankan

pesan teks, serta dapat menyajikan enkripsi dan dekripsi pesan teks dengan tepat.

Pada tahun 2020 penelitian oleh Heri Santoso, Mhd. dan Zulfansyuri Siambaton dari Univeristas Islam Negeri Sumatera Utara pada jurnal penelitian yang berjudul Aplikasi Pengamanan Ekstensi File Menggunakan Kriptografi One Time Pad (OTP) dan *Elliptic Curve Cryptography* (ECC). Penelitian ini membahas proses enkripsi (penyandian data) dan proses dekripsi (pengembalian data asli) file dengan algoritma *Elliptic Curve Cryptography* (ECC) dan One Time Pad (OTP) yang diterapkan pada sistem. Sebuah sistem yang dapat meng-enkripsi dan dekripsi sebuah file dengan implementasi algoritma *Elliptic Curve Criptography (ECC)* dan One Time Pad (OTP). Didapatkan hasil proses enkripsi *plaintext* menggunakan algoritma *One Time Pad* dapat melindungi informasi yang terdapat dalam file teks tersebut. Proses enkripsi menggunakan *One Time Pad* adalah jumlah karakter kunci harus sepanjang karakter *plaintext*, sedangkan untuk proses enkripsi menggunakan Algoritma *Elliptic Curve Cryptography (ECC)* dapat melindungi informasi yang terdapat dalam *file* teks, dengan proses enkripsi untuk mengubah satu titik ke titik yang lain sebagai *ciphertext*, sedangkan untuk proses dekripsi mengubah satu titik (chipertext) ke titik semula. Namun pada penelitian ini algoritma *Elliptic Curve Cryptography* dilakukan pengujian enkripsi didapatkan hasil bahwa beberapa *file* seperti gambar dan video tidak dapat dienkripsi dengan baik.