PROPOSAL TUGAS AKHIR – EF234702

IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY DAN ADVANCED ENCRIPTION STANDARD PADA KOMUNIKASI BERKAS BINER APLIKASI MOBILE CHAT

SEJATI BAKTI RAGA

NRP 5025201007

Dosen Pembimbing

Ary Mazharuddin Shiddiqi, S.Kom., M.Comp.Sc., Ph.D.NIP

NIP 19810620 200501 1 003

Program Studi S1 Teknik Informatika

Departemen Teknik Informatika

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

Surabaya

2024

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY DAN ADVANCED ENCRIPTION STANDARD PADA KOMUNIKASI BERKAS BINER APLIKASI MOBILE CHAT

PROPOSAL TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana Komputer pada
Program Studi S-1 Teknik Informatika
Departemen Teknik Informatika
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember

Oleh : **SEJATI BAKTI RAGA**
NRP. 5025201007

Disetujui oleh Tim Penguji Proposal Tugas Akhir:

1.	Ary Mazharuddin Shiddiqi, S.Kom., M.Comp.Sc., Ph.D.	Pembimbing
2.		Ko-pembimbing
3.	Nama dan gelar penguji	Penguji
4.	Nama dan gelar penguji	Penguji
5.	Nama dan gelar penguji	Penguji

SURABAYA
Juni, 2024

APPROVAL SHEET

IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY AND ADVANCED ENCRYPTION STANDARD ALGORITHMS IN BINARY FILE COMMUNICATION FOR MOBILE CHAT APPLICATIONS

FINAL PROJECT PROPOSAL

Submitted to fulfill one of the requirements
for obtaining a degree Computer Engineering at
Undergraduate Study Program of Informatics Engineering
Department of Informatics Engineering
Faculty of Electrical and Intelligent Information Technology
Sepuluh Nopember Institute of Technology

By: **SEJATI BAKTI RAGA**
NRP. 5025201007

Approved by Final Project Proposal Examiner Team:

1.	Ary Mazharuddin Shiddiqi, S.Kom., M.Comp.Sc., Ph.D.	Advisor
2.		Co-Advisor
3.	Name of Examiner and academic title	Examiner
4.	Name of Examiner and academic title	Examiner
5.	Name of Examiner and academic title	Examiner

SURABAYA
June, 2024

IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY DAN ADVANCED ENCRIPTION STANDARD PADA KOMUNIKASI BERKAS BINER APLIKASI MOBILE CHAT

Nama Mahasiswa / NRP : SEJATI BAKTI RAGA / 5025201007
Departemen : Teknik Informatika FTEIC - ITS
Dosen Pembimbing : Ary Mazharuddin Shiddiqi, S.Kom., M.Comp.Sc., Ph.D.

Abstrak

Implementasi algoritma Elliptic Curve Cryptography (ECC) dan Advanced Encryption Standard (AES) dalam konteks komunikasi berkas biner pada aplikasi mobile chat dibahas untuk mengatasi kerentanan penyadapan dan manipulasi. Berkas biner seperti gambar, video, dan dokumen seringkali menjadi sasaran utama bagi pihak yang ingin menyadap atau memanipulasi komunikasi. Oleh karena itu, penggunaan ECC dan AES diusulkan sebagai solusi untuk mengamankan berkas-berkas tersebut. ECC dipilih karena memiliki tingkat keamanan yang tinggi sekaligus efisiensi komputasi yang baik, khususnya cocok untuk digunakan pada perangkat mobile. Sementara AES dianggap sebagai standar enkripsi simetris yang telah teruji keandalannya secara luas. Dalam implementasi yang diusulkan, kedua algoritma akan diintegrasikan ke dalam aplikasi chat mobile menggunakan kerangka kerja Flutter. Kunci enkripsi AES akan diamankan dengan ECC sebelum berkas terenkripsi dikirimkan. Selain itu, perancangan protokol pengiriman berkas yang aman antara dua pengguna aplikasi juga menjadi bagian dari pemikiran. Evaluasi kinerja protokol akan mencakup aspek kecepatan, overhead, dan keamanan, yang akan menjadi fokus analisis untuk memastikan keefektifan solusi yang diusulkan. Dengan demikian, upaya dilakukan untuk menyajikan solusi yang holistik dan terpadu untuk meningkatkan keamanan komunikasi berkas biner pada aplikasi mobile chat.

Kata kunci: Elliptic Curve Cryptography, Advanced Encryption Standard, mobile chat application, secure file transfer protocol

IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY AND ADVANCED ENCRYPTION STANDARD ALGORITHMS IN BINARY FILE COMMUNICATION FOR MOBILE CHAT APPLICATIONS

Student Name / NRP: SEJATI BAKTI RAGA / 5025201007
Department : Informatics Engineering FTEIC - ITS
Advisor : Ary Mazharuddin Shiddiqi, S.Kom., M.Comp.Sc., Ph.D.

Abstract

The implementation of Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) in the context of binary file communication on mobile chat applications is discussed to address vulnerabilities to interception and manipulation. Binary files such as images, videos, and documents are often prime targets for those seeking to intercept or manipulate communication. Hence, the use of ECC and AES is proposed as a solution to secure these files. ECC is chosen for its high level of security combined with good computational efficiency, particularly suitable for mobile devices. Meanwhile, AES is regarded as a widely tested standard for symmetric encryption. In the proposed implementation, both algorithms will be integrated into the mobile chat application using the Flutter framework. AES encryption keys will be secured with ECC before encrypted files are transmitted. Additionally, the design of a secure file transfer protocol between two application users is also considered. Performance evaluation of the protocol will cover aspects such as speed, overhead, and security, which will be the focus of analysis to ensure the effectiveness of the proposed solution. Thus, efforts are made to present a holistic and integrated solution to enhance the security of binary file communication on mobile chat applications.

Kata kunci: Elliptic Curve Cryptography, Advanced Encryption Standard, mobile chat application, secure file transfer protocol

DAFTAR ISI

DAFTAR GAMBAR/GRAFIK/DIAGRAM

DAFTAR TABEL

BAB I PENDAHULUAN

1.1 Latar belakang

Revolusi digital telah merambah ke ranah komunikasi interpersonal, ditandai dengan maraknya aplikasi mobile chat. Platform perpesanan instan ini memungkinkan pengguna untuk saling bertukar beragam data, dari teks sederhana hingga berkas biner seperti gambar, video, dan dokumen. Kecepatan dan kemudahannya menjadikan aplikasi chat sebagai tulang punggung komunikasi modern.

Namun, di balik kemudahan tersebut, mengintai bayang-bayang kelam keamanan informasi. Berkas-berkas yang melintas melalui jaringan internet rentan terhadap serangan siber seperti penyadapan, penggondolan data, dan manipulasi berkas. Risiko ini kian besar mengingat sifat terbuka dan dinamis dari infrastruktur dunia maya.

Keadaan ini menyoroti urgensi sistem keamanan yang mumpuni untuk melindungi kerahasiaan dan integritas berkas biner yang dibagikan melalui aplikasi mobile chat. Menjamin bahwa pesan yang dikirim sampai ke penerima yang dituju dalam bentuk aslinya tanpa modifikasi atau pengintipan oleh pihak-pihak yang tidak berkepentingan, merupakan landasan kepercayaan dalam komunikasi digital.

Disinilah kriptografi memainkan peran krusial. Sebagai ilmu dan seni mengamankan informasi, kriptografi menawarkan berbagai mekanisme untuk menyandikan dan melindungi data. Dari sekian banyak algoritma kriptografi, Elliptic Curve Cryptography (ECC) dan Advanced Encryption Standard (AES) mencuat sebagai solusi potensial untuk menjawab tantangan keamanan komunikasi berkas biner dalam aplikasi mobile chat.

ECC menawarkan kombinasi unik antara efisiensi komputasi dan tingkat keamanan tinggi. Hal ini ditandai dengan penggunaan kunci kriptografi yang relatif pendek dibandingkan algoritma sejenis lainnya, namun tetap menjamin ketahanan terhadap serangan pemecahan kode. Efisiensi ini menjadi sangat krusial dalam dunia perangkat mobile yang memiliki keterbatasan komputasi dan daya.

Di sisi lain, AES merupakan standar enkripsi simetri yang diakui secara internasional dan telah teruji ketahanannya terhadap berbagai serangan kriptografi. Algoritma ini menjamin kerahasiaan data dengan mekanisme enkripsi yang kuat dan terstandarisasi.

Dengan menggabungkan kekuatan ECC dan AES, penelitian ini bertujuan untuk mengembangkan sistem keamanan komunikasi berkas biner yang efektif untuk aplikasi mobile chat. Implementasi kedua algoritma ini diharapkan dapat membentuk lapisan pertahanan yang kokoh, menjaga agar pesan-pesan sensitif dan berkas-berkas penting tidak jatuh ke tangan yang salah.

Penelitian ini tidak hanya berkutat pada aspek teknis kriptografi, tetapi juga mempertimbangkan faktor-faktor seperti efisiensi komputasi, kebutuhan daya, dan kemudahan penggunaan dalam konteks aplikasi mobile. Mengingat keterbatasan sumber daya di perangkat mobile, pemilihan dan optimalisasi algoritma menjadi aspek krusial untuk menjamin kelancaran dan kesinambungan komunikasi yang aman.

Melalui penelitian ini, diharapkan dapat dikembangkan solusi keamanan komunikasi berkas biner yang efektif, efisien, dan mudah digunakan untuk aplikasi mobile chat. Dengan demikian, pengguna dapat menikmati kemudahan dan kecepatan komunikasi digital tanpa mengorbankan privasi dan keamanan data mereka.

1.2 Rumusan Permasalahan

Berdasarkan latar belakang di atas, maka dapat ditarik rumusan masalah sebagai berikut:

1. Apakah implementasi gabungan algoritma ECC dan AES dapat meningkatkan keamanan komunikasi berkas biner pada aplikasi mobile chat?
2. Bagaimana cara mengoptimalkan implementasi ECC dan AES agar efisien dalam hal komputasi dan konsumsi daya pada perangkat mobile?
3. Bagaimana tingkat efektivitas dan kemudahan penggunaan sistem keamanan yang dikembangkan dalam penelitian ini?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Implementasi algoritma menggunakan bahasa Python dan Scala.
2. Pembuatan sistem hanya berfokus pada proses *debugging* dan *generate* test input bukan pada program yang test inputnya akan didebug dan di-*generate*.
3. Test input berupa *Text* yang menyatukan beberapa kolom yang dibutuhkan.

1.4 Tujuan

Tujuan penelitian ini adalah sebagai berikut:

1. Mengimplementasikan enkripsi berkas biner menggunakan AES pada aplikasi mobile chat Flutter.
2. Menggunakan ECC untuk mengamankan kunci AES yang digunakan dalam proses enkripsi berkas.
3. Merancang protokol pengiriman berkas terenkripsi antara dua pihak pada aplikasi mobile chat.

1.5 Manfaat

Manfaat penelitian ini adalah sebagai berikut:

1. Meningkatkan keamanan komunikasi berkas biner pada aplikasi mobile chat dengan menerapkan ECC dan AES.
2. Memberikan rekomendasi implementasi ECC dan AES yang efisien untuk aplikasi mobile chat.
3. Mengevaluasi efektivitas dan kemudahan penggunaan ECC dan AES pada aplikasi mobile chat.
4. Hasil penelitian dapat menjadi acuan bagi pengembang aplikasi mobile chat dalam menerapkan sistem keamanan.
5. Rancangan protokol pengiriman berkas terenkripsi antar pengguna dapat diadaptasi pada aplikasi mobile chat sesungguhnya.

BAB II TINJAUAN PUSTAKA

2.1 Penelitian Terkait

2.1.1 Pembuatan Aplikasi Chat Messenger Menggunakan Advanced Encryption Standard (AES) dan Firebase Realtime Database

Penelitian yang dilakukan oleh Vinsensius Arka Biwara Adi dan rekan-rekannya berfokus pada pengembangan keamanan aplikasi chat messenger. Mereka menghadapi tantangan dalam mengamankan pesan, terutama terkait dengan pesan yang rentan disadap atau dimanipulasi. Untuk mengatasi masalah ini, penelitian ini memperkenalkan metode baru yang menggabungkan Advanced Encryption Standard (AES) dan Firebase Realtime Database. Pesan akan dienkripsi terlebih dahulu menggunakan AES sebelum dikirim, sehingga pesan terlindungi saat transit. Firebase Realtime Database digunakan untuk menyimpan pesan yang terenkripsi. Hasil dari penelitian ini adalah peningkatan keamanan pesan chat, dengan pesan yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dengan demikian, penelitian ini berpotensi memberikan manfaat besar dalam mengamankan kerahasiaan pesan pada aplikasi chat messenger. [1]

2.1.2 Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android

Penelitian yang dilakukan oleh Danang H. Sulaksono dan rekan-rekannya berfokus pada pengembangan keamanan aplikasi chatting Android. Mereka menghadapi tantangan dalam mengamankan pesan dan gambar yang dikirimkan, yang rentan dibaca oleh pihak yang tidak berwenang. Untuk mengatasi masalah ini, penelitian ini memperkenalkan metode Elliptic Curve Cryptography (ECC). Pesan dan gambar akan dienkripsi terlebih dahulu menggunakan ECC sebelum dikirim, sehingga isinya terlindungi saat transit. Hasil dari penelitian ini adalah peningkatan keamanan dan kerahasiaan pesan pada aplikasi chatting Android, dengan nilai Avalanche Effect rata-rata sebesar 79,89. Dengan demikian, penelitian ini berpotensi memberikan manfaat besar dalam menjaga kerahasiaan pesan dan gambar pada aplikasi chatting berbasis Android. [2]

2.1.3 Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi

Penelitian yang dilakukan oleh Zaenul Arif dan rekan-rekannya berfokus pada perbandingan kinerja algoritma kriptografi. Mereka menghadapi tantangan dalam menentukan algoritma terbaik untuk meningkatkan keamanan sistem informasi. Untuk mengatasi masalah ini, penelitian ini melakukan analisis perbandingan algoritma AES (simetris) dan ECC (asimetris). Kedua algoritma dievaluasi berdasarkan faktor keamanan, efisiensi, dan kemudahan implementasi. Hasil penelitian menunjukkan bahwa AES lebih cepat dan efisien memproses data, sedangkan ECC lebih aman terutama untuk komunikasi jarak jauh dan tanda tangan digital. Kesimpulannya, pemilihan algoritma harus disesuaikan dengan kebutuhan sistem informasi. Dengan demikian, penelitian ini berpotensi memberikan panduan yang bermanfaat dalam menentukan algoritma terbaik untuk meningkatkan keamanan suatu sistem informasi. [3]

2.1.4 Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)

Penelitian yang dilakukan oleh Muhammad Azhari dan rekan-rekannya berfokus pada penerapan Advanced Encryption Standard (AES) untuk meningkatkan keamanan data.

Mereka menghadapi tantangan dalam melindungi kerahasiaan dan integritas data sensitif dari penyadapan dan manipulasi. Untuk mengatasi masalah ini, penelitian ini mengimplementasikan AES dengan panjang kunci 128-bit, 192-bit, dan 256-bit. AES melakukan enkripsi data menggunakan transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Sedangkan dekripsi menggunakan operasi kebalikan, kecuali AddRoundKey. Hasilnya, AES mampu menyediakan tingkat keamanan tinggi untuk melindungi kerahasiaan dan integritas berbagai jenis data. Dengan demikian, penelitian ini berpotensi memberikan manfaat besar dalam mengamankan data sensitif dari ancaman keamanan informasi. [4]

2.1.5 Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey

Penelitian yang dilakukan oleh Shamsher Ullah dan rekan-rekannya berfokus pada penerapan Elliptic Curve (EC) untuk meningkatkan keamanan sistem informasi modern. EC merupakan teknik ECC termutakhir yang sering digunakan untuk mengamankan berbagai jaringan terbuka dan teknologi modern seperti media sosial, komputasi awan, dan Internet of Things yang rentan terhadap serangan keamanan informasi. Studi ini menyelidiki secara komprehensif berbagai konsep ilmiah, metodologi inovatif, dan implementasi terkait penggunaan ECDSA untuk otentikasi, integritas data, dan tanda tangan digital. Skema berbasis EC diklaim lebih aman dan efisien dibandingkan algoritma kriptografi seperti RSA dan Diffie-Hellman. Selain itu, penggunaannya pada komputasi terdistribusi dan jaringan asinkron terbukti memberikan manfaat signifikan dalam menjaga kerahasiaan dan otentikasi. Secara keseluruhan, penelitian ini berpotensi bermanfaat bagi akademisi dan praktisi keamanan informasi yang tertarik melakukan kajian dan analisis lebih lanjut terhadap penerapan EC untuk meningkatkan keamanan sistem informasi di era digital. [5]

2.2 Dasar Teori

2.2.1 *Algoritma Elliptic Curve Criptography (ECC)*

Elliptic Curve Cryptography (ECC) adalah metode kriptografi kunci publik berdasarkan struktur aljabar kurva elips di daerah finite, ditemukan pada tahun 1985 oleh Neal Koblitz dan Victor S. Miller. Kurva elips juga diterapkan dalam algoritma pemaktoran integer, seperti Lenstra Elliptic Curve Factorization, yang memiliki aplikasi kriptografi. Pada ECC, parameter-parameter seperti a, b, bilangan prima p, dan titik generator G harus ditentukan sebelumnya. Proses enkripsi melibatkan langkah-langkah seperti pembangkitan kunci privat dan publik oleh Aktor 1, enkripsi pesan oleh Aktor 2, dan deskripsi oleh Aktor 1. ECC memanfaatkan sifat matematis kurva elips untuk menyediakan keamanan kunci publik tinggi dan tahan terhadap serangan siber. [5]

2.2.2 *Algoritma Advanced Encription Standard (AES)*

Advanced Encryption Standard (AES) dipilih sebagai standar algoritma kriptografi internasional pada tahun 2000 setelah melewati kontes pemilihan sebagai pengganti DES. Dari lima calon yang tersisa, Rijndael, dikembangkan oleh Dr. Vincent Rijmen dan Dr. Joan Daemen, terpilih karena kombinasi keamanan dan efisiensi implementasinya. Nama "Rijndael" sendiri berasal dari gabungan nama kedua penemunya. AES menggunakan struktur kunci simetris dan memiliki panjang kunci yang dapat dipilih (128-bit, 192-bit, atau 256-bit), menawarkan kecepatan dan ketahanan tinggi terhadap berbagai serangan, sehingga menjadi salah satu algoritma enkripsi paling banyak digunakan secara global. [1]

2.2.3 *Framework Flutter*

Flutter, sebuah kerangka kerja lintas platform yang dirancang untuk membangun aplikasi mobile berkinerja tinggi, diperkenalkan secara publik oleh Google pada tahun 2016 dan dimaksudkan untuk digunakan dalam pengembangan aplikasi tidak hanya untuk Android dan iOS tetapi juga untuk sistem operasi Fuchsia. Ini dipilih oleh Google sebagai kerangka kerja tingkat aplikasi untuk sistem operasi generasi berikutnya. Keunikan Flutter terletak pada ketergantungannya pada widget OEM perangkat daripada tampilan web, menggunakan mesin pengurai berkinerja tinggi untuk setiap komponen tampilan. Pendekatan ini memungkinkan pembangunan aplikasi yang sekinerja mungkin dengan aplikasi native. Dari segi arsitektur, kode C atau C++ mesin mengalami kompilasi dengan Android NDK dan LLVM untuk iOS, sedangkan selama proses ini, kode Dart dikompilasi menjadi kode native. Flutter menonjolkan peningkatan siklus pengembangan yang signifikan dengan fitur Stateful hot reload-nya, memungkinkan pengiriman kode sumber yang diperbarui ke Dart Virtual Machine tanpa mengubah struktur internal aplikasi. Akibatnya, transisi dan tindakan dalam aplikasi tetap utuh setelah pengisian ulang panas. Kombinasi unik ini menempatkan Flutter sebagai kerangka kerja yang fleksibel untuk pengembangan efisien aplikasi mobile berkinerja tinggi, dapat disesuaikan baik untuk platform Android dan iOS saat ini maupun sistem masa depan potensial seperti Fuchsia. [6]

2.2.4 Bahasa Pemrograman Dart

Dalam kerangka kerja Flutter, setiap aplikasi ditulis dengan menggunakan Dart, sebuah bahasa pemrograman yang dikembangkan dan dikelola oleh Google. Dart, awalnya diciptakan sebagai pengganti potensial untuk JavaScript, telah menjadi populer di dalam Google, terbukti mampu mengembangkan aplikasi web berskala besar seperti AdWords. Dart mengadopsi fitur-fitur kunci dari standar selanjutnya JavaScript (ES7), termasuk kata kunci "async" dan "await", sehingga sejalan dengan praktik pemrograman modern. Meskipun memiliki latar belakang sebagai pengganti JavaScript, Dart menggunakan sintaksis mirip Java untuk memudahkan pengembang yang tidak akrab dengan JavaScript. Secara khusus, aplikasi Flutter memperbarui pohon tampilan pada setiap frame baru, berbeda dari sistem lain yang menggunakan tampilan reaktif. Meskipun pendekatan ini dapat menyebabkan pembuatan banyak objek yang bertahan hanya satu frame, desain modern Dart menangani skenario ini secara efisien melalui "Generational Garbage Collection" di tingkat memori. [6]

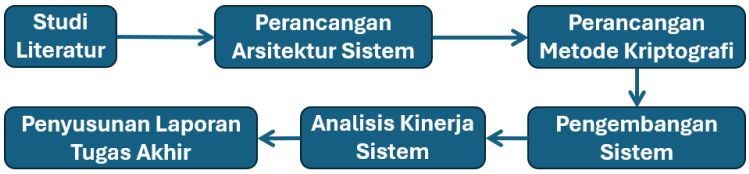
2.2.5 Firebase

Firebase menyediakan backend-as-a-service dengan fitur autentikasi pengguna, basis data realtime, push notification, remote configuration, dan analytics yang sangat bermanfaat untuk meningkatkan keamanan, kehandalan, dan pengalaman pengguna pada aplikasi chat messenger. Layanan ini memastikan hanya pengguna terverifikasi yang dapat mengakses aplikasi chat, menyimpan data penting secara realtime, serta mengirimkan pesan dan notifikasi meski aplikasi chat tidak sedang aktif. Dengan memanfaatkan berbagai fitur Firebase secara menyeluruh, aplikasi chat messenger dapat dibuat lebih aman, handal, dan memberikan pengalaman terbaik bagi penggunanya. [1]

BAB III METODOLOGI

3.1 Metode yang dirancang

Metode yang dirancang pada penelitian ini sebagaimana ditunjukkan pada Gambar 3.1



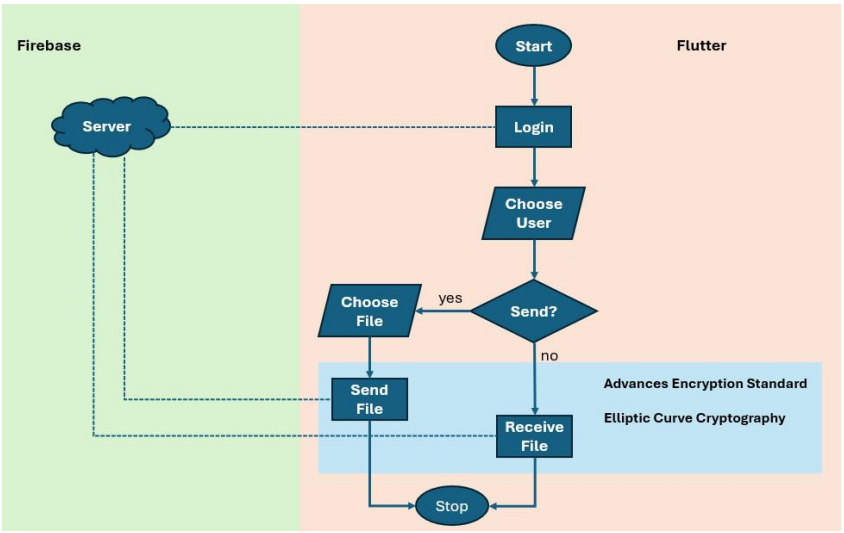
Gambar 3 1 Diagram Alir Metode Penelitian

- Studi Literatur

  Pada tahap ini dilakukan riset studi literatur mengenai konsep dan permasalahan yang menyangkut Algoritma Elliptic Curve Criptography, Algoritma Advanced Encription Standard, Kerangka Kerja Fluttern dan Bahasa Pemrograman Dart melalui buku, internet, jurnal-jurnal ilmiah yang berkaitan.

- Perancangan Arsitektur Sistem

  Tahap perancangan arsitektur sistem dilakukan dengan mengombinasikan dasar teori pada bab 2. Perancangan metode akan dimulai dari proses penerapan algoritma ECC dan AES menggunakan Bahasa pemrograman Dart. Algoritma tersebut kemudian dikombinasikan dan diterapkan pada aplikasi yang dibuat menggunakan kerangka kerja Flutter, Firebase, hingga penggabungan keseluruhan proses menjadi satu arsitektur utuh yang dapat di lihat pada Gambar 3.2

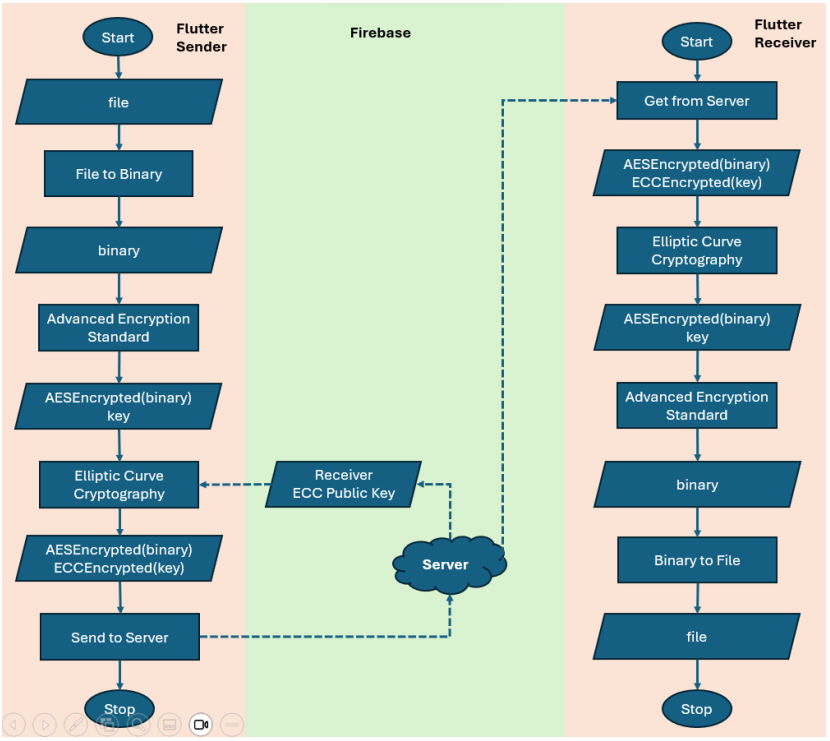


Gambar 3 2 Rancangan Arsitektur Sistem

- Perancangan Metode Kriptografi

  Tahap perancangan metode kriptografi dilakukan dengan membuat algoritma pengiriman dan penerimaan file yang akan menerapkan algoritma enkripsi AES dan ECC. Pada awalnya file akan diubah menjadi bentuk binary kemudian akan dienkripsi menggunakan AES. Kemudian key AES akan dienkripsi dengan algoritma ECC menggunakan public key dari penerima yang diakses melalui Firebase. Setelah itu file binary dan key AES yang terenkripsi akan dikirim, kemudian penerima akan mendekripsi key AES dengan algoritma ECC menggunakan public dan private key miliknya. Sedangkan file binary yang terenkripsi akan didekripsi menggunakan key

AES yang sudah didekripsi sebelumnya. File binary kemudian diubah menjadi bentuk file dan ditampilkan ke dalam aplikasi Flutter. Tahap ini dapat ditunjukkan melalui Gambar 3.3.



Gambar 3 3 Rancangan Metode Kriptografi

- Pengembangan Sistem

  Pengembangan sistem dilakukan dengan menerapkan algoritma solusi yang dirancang pada subbab perancangan arsitektur sistem. Untuk keseluruhan sistem yang dihasilkan pada perancangan arsitektur sistem akan menggunakan bahasa pemrograman dart dengan kerangka kerja Flutter, sedangkan untuk bagian backend akan menggunakan firebase untuk menyimpan public key ECC dari masing-masing user dan untuk kebutuhan autentikasi.

- Analisis Kinerja Sistem

  Analisis kinerja sistem yang akan dilakukan pada penelitian ini ada dua, yaitu yaitu uji kinerja dan uji keamanan. Uji kinerja pada penelitian ini meliputi pengujian kecepatan enkripsi dan dekripsi berkas serta analisis overhead yang ditambahkan oleh ECC dan AES pada aplikasi mobile chat. Sedangkan uji keamanan mencakup evaluasi keamanan protokol yang diimplementasikan dan uji penetrasi untuk memastikan ketangguhan sistem terhadap serangan. Enkripsi dan dekripsi berkas akan diuji kecepatannya untuk menganalisis kinerja sistem. Overhead ECC dan AES juga akan dianalisis pengaruhnya terhadap kinerja aplikasi mobile chat. Sementara itu, keamanan protokol akan dievaluasi apakah telah memenuhi standar keamanan yang ditentukan. Uji penetrasi juga akan dilakukan dengan meluncurkan serangan untuk memastikan sistem mampu bertahan. Dengan demikian diharapkan didapatkan analisis menyeluruh terhadap kinerja dan keamanan sistem.

- Penyusunan Laporan Tugas Akhir

  Tahap ini merupakan tahap akhir dari penelitian ini yaitu penyusunan laporan dalam bentuk buku tugas akhir yang menjelaskan dasar teori dan metode yang

digunakan dalam tugas akhir ini serta hasil implementasi yang telah dibuat. Sistematika penulisan buku tugas akhir secara garis besar antara lain :

1. Pendahuluan
    a. Latar Belakang
    b. Rumusan Masalah
    c. Batasan Tugas Akhir
    d. Tujuan
    e. Metodologi
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

3.2 Peralatan pendukung

Terdapat beberapa peralatan hardware dan software pendukung yang digunakan untuk pengembangan sistem pada Tugas Akhir ini yang dapat dilihat sebagai berikut:

- Laptop Lenovo ideapad Slim 3
- Visual Studio Code
- Android Studio
- Flutter
- Firebase

3.3 Rencana Implementasi dan Uji Coba

Dalam membuat Tugas Akhir ini, terdapat beberapa proses yang perlu dilakukan sesuai pada Gambar 3.4.

Gambar 3 4 Diagram Alir Rencana Implementasi dan Uji Coba

Rencana uji coba yang akan dilakukan pada penelitian ini yaitu dengan melakukan build aplikasi pada dua perangkat mobile berbeda dan melakukan transaksi file menggunakan aplikasi tersebut. Setelah itu akan dilakukan proses analisis kinerja dan keamanan pada file yang ditransaksikan.

JADWAL KEGIATAN

NO	Nama Kegiatan	Minggu ke-													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Studi Literatur														
2	Perancangan Arsitektur Sistem														
3	Perancangan Metode Kriptografi														
4	Pengembangan Sistem														
5	Analisis Kinerja Sistem														
6	Penyusunan Laporan Tugas Akhir														

Tabel 3 1 Rencana Kegiatan

DAFTAR PUSTAKA

[1] V. A. B. Adi, R. A. T. Sudalyo and A. Baraja, "Pembuatan Aplikasi Chat Messenger Menggunakan Advanced Encryption Standard (AES) dan Firebase Realtime Database," in *Seminar Nasional Teknologi Informasi dan Komunikasi*, 2023.

[2] D. H. Sulaksono, C. N. Prabiantissa, G. E. Yuliastuti and A. R. Taqwa, "Implementasi Kriptografi dengan Metode Elliptic Curve Cryptography (ECC) untuk Aplikasi Chatting Berbasis Android," in *Seminar Nasional Sains dan Teknologi Terapan IX*, Surabaya, 2021.

[3] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *JTSI*, 2023.

[4] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer,* 2022.

[5] S. Ullah, Z. Jiangbin, N. Din, M. T. Hussain, F. Ullah and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, 2023.

[6] A. Tashildar, N. Shah, R. Gala, T. Giri and P. Chavhan, "APPLICATION DEVELOPMENT USING FLUTTER," *International Research Journal of Modernization in Engineering Technology and Science,* 2020.