BAB I
PENDAHULUAN

1.1 Latar Belakang

Notes atau catatan yaitu kumpulan catatan dalam bentuk tulisan atau teks yang memberikan keterangan sebagai pengingat, di simpan dalam arsip atau dokumen. informasi tersebut dapat di rekam dalam komputer atau smartphone.

Di era 5.0 digital dunia teknologi berkembang begitu cepat, khususnya dalam berbasis android. Maka dalam tingkat keamanan dalam data juga dibutuhkan karena untuk menyimpan sebuah data tanpa perlu dengan buku atau pena. Sekarang bisa menyimpan, mencatat hanya dengan smartphone, dan setiap data akan terjaga kerahasiaan informasi catatan dengan aman tanpa perlu khawatir data di curi oleh orang lain.

Di dalam sebuah hadist sudah menyinggung untuk menjaga privasi yaitu Dari Abu Hurairah *rodhiyallahu'anhu* berkata, bahwa beliau mendengar Rasulullah *shallallahu'alaihi wa sallam* bersabda :

لَوِ اطَّلَعَ فِي بَيْتِكَ أَحَدٌ، وَلَمْ تَأْذَنْ لَهُ، خَذَفْتَهُ بِحَصَاةٍ، فَفَقَأْتَ عَيْنَهُ مَا كَانَ عَلَيْكَ مِنْ جُنَاحٍ

Seandainya ada orang mengintip rumahmu, dan dia tidak meminta izin kepadamu, kemudian kamu melemparnya dengan kerikil sehingga tercungkil matanya, maka tiada dosa atasmu. (HR. Bukhari, hadist no. 6888).

Oleh karena itu di perlukan suatu penjagaan atau sebuah sistem keamanan yang akan menjaga infomasi dalam catatan tersebut yaitu aplikasi note menggunakan kriptografi AES. Seperti itu, data catatan yang di miliki dapat di acak dan di dekodekan secara eksklusif dengan kunci (key) yang di tempatkan sehingga tidak ada seorang pun kecuali klien yang dapat mengetahui data catatan tersebut. Sejalan dengan itu, salah satunya menerapkan perhitungan kriptografi AES(*Advanced Encryption Standard*) Rijndael.

Kriptografi adalah ilmu atau keahlian menjaga keamanan pesan atau data yang akan di peroleh secara tepat. Perhitungan kriptografi di bagi menjadi 3 bagian dengan berdasarkan kunci, khususnya perhitungan simetris, perhitungan hilter, kilter, dan kemampuan hash. Perhitungan simetris adalah contoh perhitungan dan menggunakan kunci simetris termasuk *Data Encryption Standard* (DES), *International Data Encryption Algoritm* (IDEA), *Advanced Encryption Standard* (AES), *One Time Pad* (OPT) RC2,RC3,RC4,RC5,DAN RC6 dan lainnya.. (Kharisma et al., 2017)

Kriptografi AES (*Advanced Encryption Standard*) merupakan perhitungan substitusi *Data Encryption Standard* (DES) dengan alasan telah habis masa legitimasinya dari faktor keamanan. Pada bulan Maret 2001, perhitungan baru Rjindael di tetapkan sebagai AES oleh *National Institute of Standard and Technology* (NIST). (Winarno et al., 2012)

Algoritma Rijndael terpilih sebagai perhitungan yang mengalahkan 5 finalis berbeda yang di pilih oleh NIST. AES di pilih sebagai pengganti algoritma DES karena bergantung pada 3 ukuran utama, khususnya keamanan biaya, dan kualitas serta pelaksanaannya. Keamanan adalah hal yang paling mendasar langkah-langkah ini, sehingga algoritma AES dapat menahan berbagai jenis serangan yang di ketahui atau tidak di ketahui. Selain itu, dalam aplikasi peralatan dan pemrograman, algoritma AES Rijndael harus menarik dan produktif saat berjalan pada tahapan yang berbeda dari 8 digit hingga 64 bit. (Winarno et al., 2012)

Android adalah kerangka kerja untuk ponsel mengingat linux yang terdiri dari middleware dan aplikasi. Android merupakan pangungg terbuka bagi para development untuk membuat aplikasi. Android juga memiliki platform yang begitu lengkap dalam sistem operasi, aplikasi, dan tool pengembang, serta dukungan tinggi dari pada komunitas *open source* di dunia. (Kharisma et al., 2017)

Berdasarkan penelitian sebelumnya telah membahas tentang enkripsi kriptografi AES berbasis android yaitu (H. Kridalaksana et al., 2018) dengan judul "Aplikasi Pengaman SMS Dengan Metode Kriptografi *Advanced Encryption Standard* (Aes) 128 Berbasis Android" denga tujuan untuk pengamanan SMS.

Sedangkan penelitian menurut (Nuari & Ratama, 2020) untuk memiliki opsi untuk meningkatkan dan memperluas keamanan informasi, para ahli merencanakan aplikasi keamanan infromasi dengan algoritma kriptografi AES (Advanced Encryption Standard) 12 bit dengan SDLC.

Penelitian menurut (Dian Widyawan, 2021) pada penelitian ini berkontribusi dalam mengamankan teks berbasis web menggunakan AES-128 bit di Komite Nasional Keselamatan Transportasi. Jadi dapat membuat aplikasi untuk mengamankan teks catatan dengan metode AES-128 berbasis web.

Berdasarkan perbedaan dari beberapa hasil penelitian yang di kemukakan di atas, maka dengan itu penulis tertarik untuk melakukan penelitian dengan objek yang berbeda dan tetap dengan berbasis android, maka dalam penelitian ini diangkatlah judul **"Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) Rijndael Dalam Keamanan Teks Catatan Berbasis Android"**

1.2 Rumusan Masalah

Berdasarkan landasan permasalahan tersebut, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana Mengimplementasikan Algoritma Kriptografi AES (*Advanced Encryption Standard*) Rijndael dalam keamanan teks catatan berbasis Android ?
2. Bagaimana proses dalam sebuah keamanan notes dengan algoritma kriptografi AES (*Advanced Encryption Standard*) Rijndael dengan panjang kunci 128, 192, dan 256, serta penerapan enkripsi dengan mode operasi block cipher ?

1.3 Batasan Masalah

Untuk menghindari penyimpangan dari perkembangan agar sesuai dengan rencana masalah, maka dalam penelitian ini di batasi sebagai berikut :

1. Objek yang di gunakan dalam enkripsi atau dekripsi AES adalah sebagai teks catatan berbasis android
2. Output yang di hasilkan berupa hexadesimal pada saat di enkripsi, dan akan kembali ke teks semula pada saat di dekripsi
3. Panjang kunci memilki keterbatasan yaitu dengan 128 bit, 192 bit, dan 256 bit
4. Teks catatan di enkripsi menggunakaan mode operasi block cipher ECB (*Electronic Code Book*)
5. Teks yang ingin di enkripsi tidak terbatas
6. Menggunakan bahasa *java* berbasis android.

1.4 Tujuan Penelitian

Berdasarkan dari rumusan masalah yang telah di gambarkan, ada beberapa tujuan yang ingin di capai dalam tinjauan ini, yaitu :

1. Untuk mengimplementasikan Algoritma Kriptografi AES (*Advanced Encryption Standard*) Rijndael dalam keamanan teks catatan berbasis Android
2. Untuk membuat sebuah keamanan teks catatan dengan kriptografi AES (*Advanced Encryption Standard*) Rijndael berbasis android

1.5 Manfaat Penelitian

Adapun manfaat yang dapat di peroleh dari penelitian yang di lakukan adalah sebagai berikut :

1. Dapat meningkatkan keamanan sebuah teks catatan berbasis android
2. Dapat di gunakan di semua kalangan, untuk dapat mengamankan data atau teks dengan kunci 128 bit, 192 bit, dan 256 bit.
3. Dapat di gunakan sebagai referensi membaca bagi setiap individu yang ingin menggunakan atau mengenal perhitungan kriptografi AES (Advanced Encryption Standard) Rijndael
4. Dapat mengembangkan pengetahuan algoritma kriptografi AES (*Advanced Encryption Standard*) Rijndael
5. Mudah di akses untuk mengenkripsi file ke dalam sebuah android