BAB 1
PENDAHULUAN

1.1 Latar Belakang

Saat ini, mayoritas orang menggunakan telepon pintar tidak hanya lagi untuk berkomunikasi atau bertukar informasi saja, melainkan juga digunakan sebagai penyimpanan informasi pribadi atau pekerjaan mereka. Kemudahan serta kenyamanan yang diberikan dari kemajuan teknologi tersebut membuat para pengguna sering kali melupakan aspek keamanannya. Kondisi ini cukup berbahaya karena rentan terhadap ancaman pencurian dan pemindaian informasi penting.

Salah satu cara yang efektif untuk melindungi data adalah melalui penggunaan kriptografi (Hermawan dkk., 2021) . Kriptografi adalah seni penyandian informasi untuk menjaga keutuhan data (Nasution & Triandi, 2021; Pasaribu dkk., 2018). Enkripsi dilakukan untuk mengacak informasi agar pihak lain selain penerima tidak bisa mengakses ataupun membaca, sehingga tetap terjaga keamanan dan kerahasiaannya sampai ke penerima, dilanjutkan dengan proses dekripsi yang mengembalikan informasi acak ke awal sehingga bisa diakses dan dibaca oleh si penerima.

Untuk melakukan proses penyandian, dibutuhkan algoritma penyusun sebagai pemrosesan mengacak data menjadi pesan rahasia. Algoritma kriptografi terus berkembang pesat hingga saat ini yang disebabkan oleh algoritma terdahulu sudah berhasil dipecahkan (Siringoringo, 2020) . Banyak algoritma kriptografi modern yang bermunculan untuk melakukan pengamanan suatu informasi, di antaranya adalah algoritma *Advanced Encryption Standard* (AES) dan algoritma Rivest Shamir Adleman (RSA). Karena kedua algoritma mempunyai kelebihan dan kekurangan maka akan dilakukan kombinasi antara algoritma AES dan algoritma RSA supaya tahapan keamanan yang dihasilkan bertambah kuat.

Algoritma simetris merupakan salah satu kategori kunci pada ilmu kriptografi, dimana algoritma AES hanya memakai satu kunci untuk proses enkripsi maupun dekripsi (Dr Asha Ambhaikar, 2021) . Algoritma AES memiliki tiga jenis kunci dengan jumlah putaran yang berbeda yaitu 128 bit dengan perputaran paling kecil, 192 bit, dan 256 bit yang memiliki puataran paling besar (Fauziah dkk., 2018; Ramadani & Sauda, 2020) . Penyandian AES menggunakan proses berulang (*round*) yang ditentukan pada panjang kunci yang diterapkan (Pattanavichai, 2022) . Sedangkan algoritma asimetris berbeda dengan simetris, karena jenis algoritma memiliki dua kunci pada proses penyandian, algoritma RSA termasuk pada

kategori ini. Kunci yang dipakai pada enkripsi bersifat tidak tersembunyi (dilihat bersama-sama), sedangkan dekripsi bersifat disembunyikan (kunci privat). Dengan demikian, data yang disandikan hanya dapat dibuka oleh orang yang mempunyai kunci privat (G. Chaloop & Z. Abdullah, 2022; Sadikin & Wardhani, 2016).

Berdasarkan paparan dan permasalahan yang didapati dari latar belakang, maka penulis di skripsi ini akan membuat implementasi kombinasi dua algoritma antara kategori kunci kriptografi simetris AES dan asimetris RSA, pada pengamanan dokumen dengan melakukan penyandian proses enkripsi dan dekripsi pada aplikasi dengan sistem operasi Android.

1.2 Rumusan Masalah

Didapatkan sejumlah masalah dari pemaparan latar belakang, dengan penjabaran sebagai berikut:

a. Bagaimana menyiapkan dan mengembangkan aplikasi enkripsi dan dekripsi dokumen pada sistem operasi android?
b. Bagaimana algoritma AES, algoritma RSA, dan kombinasi AES dan RSA melakukan enkripsi dan dekripsi data?
c. Bagaimana penerapan kombinasi algoritma AES dan algoritma RSA dalam mengamankan dokumen?
d. Bagaimana kecepatan algoritma AES, algoritma RSA, serta kombinasi antara algoritma AES dan RSA pada aplikasi pengamanan dokumen berbasis android?

1.3 Batasan Masalah

a. Algoritma kriptografi yang dipakai adalah algoritma AES 256 bit dan algoritma RSA 2048 bit
b. Program aplikasi ini hanya dapat dijalankan pada sistem operasi Android
c. Data yang diuji untuk proses operasi enkripsi dan operasi dekripsi berupa dokumen tulisan
d. Bahasa pemrograman Kotlin yang dipakai serta IDE *Android Studio* dalam mengembangkan aplikasi.
e. Dokumen yang diizinkan untuk dienkripsi terdiri dari (*.pdf, *.docx, *.doc, *.xls, *.xlsx, *.ppt, *pptx, *.csv)
f. Jenis file dokumen yang hanya dapat didekripsi berupa (*.enc)

1.4 Tujuan

a. Untuk mengetahui cara merancang dan membangun aplikasi enkripsi dan dekripsi dokumen pada sistem operasi android.
b. Untuk mengetahui proses enkode dan dekode data memakai algoritma AES, algoritma RSA, serta kombinasi AES dan RSA
c. Untuk mengetahui penerapan kombinasi dari algoritma AES dan algoritma RSA dalam mengamankan dokumen.
d. Untuk mengetahui waktu yang dibutuhkan oleh algoritma AES, algoritma RSA, serta kombinasi antara algoritma AES dan RSA pada aplikasi pengamanan dokumen berbasis android.

1.5 Kontribusi

Adapun kontribusi yang diberikan dari penelitian ini berupa:

a. Penelitian dilakukan untuk memberikan manfaat dalam keamanan data dari segala ancaman kejahatan siber bagi para pengguna telepon pintar berbasis Android.
b. Sebagai sarana pengembangan keilmuan informatika dalam bidang kriptografi dan android, serta kemampuan dalam membangun suatu aplikasi enkode dan dekode dengan mengimplementasikan algoritma kunci simetris AES dan algoritma kunci asimetris RSA.