

# **BAB 1**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Teknologi enkripsi pada masa sekarang sangat diperlukan untuk melindungi data, baik itu data pribadi maupun data organisasi. Dalam konteks untuk melindungi data pribadi, dibutuhkan aplikasi yang dapat melindungi data pribadi agar tidak mudah dibuka atau dilihat oleh orang lain. Dalam penelitian kali ini akan dibuat sebuah aplikasi pengamanan data berupa pesan teks, dokumen, teks, gambar dan video menggunakan teknik enkripsi dan dekripsi. Metode algoritma yang dipakai adalah algoritma Rijndael yang dijalankan pada sistem operasi android. Algoritma Rijndael ditetapkan oleh NIST (National Institute of Standards and Technology) sebagai standar enkripsi AES (Advanced Encryption Standard).

Teknik enkripsi dapat mengamankan data karena data akan berubah menjadi tidak terbaca sesuai dengan aslinya. Data tersebut dapat dibaca apabila sudah didekripsi menggunakan kunci yang benar. Aplikasi enkripsi dan dekripsi ini akan membuat data menjadi lebih aman dari pihak lain yang tidak mempunyai ijin untuk mengakses data tersebut.

Teknologi perangkat mobile kini sudah digunakan oleh banyak orang di dunia. Perangkat mobile digunakan banyak orang karena mempunyai mobilitas dan praktis dalam penggunaannya. Banyak perangkat mobile saat ini sudah mempunyai teknologi yang mutakhir. Perangkat mobile saat ini dapat membantu aktifitas menjadi lebih efektif dan efisien. Sistem operasi dalam perangkat mobile selalu berkembang. Sistem operasi perangkat mobile yang sedang populer saat ini adalah sistem operasi android. Banyak pengembang ikut serta dalam membangun perangkat lunak berbasis android dikarenakan android adalah sistem operasi yang dikembangkan secara terbuka (open source).

Perangkat mobile berbasis android tidak hanya digunakan untuk komunikasi saja. Banyak kegunaan lain dari perangkat mobile berbasis android yaitu pengambilan foto/video, mendengarkan musik, membuat file dokumen, menyimpan data, dan

sebagainya. Kemampuan perangkat mobile android dalam hal kapasitas penyimpanan data semakin meningkat. Banyak data-data penting yang hanya boleh diketahui oleh pemiliknya dan seijin pemiliknya saja. Hal ini menjadi suatu prioritas karena data-data penting yang tidak dilindungi dapat dibuka, dibajak, atau mungkin disebarluaskan oleh pihak lain yang tidak memiliki ijin dari pemilik data.

Berdasarkan penjabaran umum diatas, maka pada penelitian ini akan dilakukan pembuatan aplikasi enkripsi dan dekripsi file dan teks menggunakan AES 256 dan SHA 256 yang diterapkan pada sistem operasi android.

## 1.2 Rumusan Masalah

Di dalam penulisan ini didapatkan beberapa rumusan masalah yang didapat yaitu:

- a. Bagaimana membangun aplikasi pengamanan file dan pesan teks menggunakan AES 256 dan SHA 256 berbasis android?
- b. Apakah aplikasi pengamanan file dan pesan teks ini dapat diterapkan menggunakan AES 256 dan SHA 256 berbasis android?
- c. Apakah aplikasi pengamanan file dan pesan teks menggunakan AES 256 dan SHA 256 dapat mengamankan fiile dan teks dengan baik?

## 1.3 Batasan Masalah

Adapun batasan masalah dalam mengimplementasikan aplikasi enkripsi dan dekripsi file dan teks menggunakan AES 256 dan SHA 256 berbasis android. Pembatasan tersebut dijelaskan di bawah ini :

- a. Proses enkripsi dan dekripsi menggunakan AES (Advanced Encryption Standard) dengan panjang kunci 256 bit.
- b. Untuk pemasukan kunci, dilakukan proses hashing menggunakan SHA 256 agar dapat menghasilkan kunci 256 bit.
- c. Aplikasi enkripsi dan dekripsi ini mencangkup data yang berjenis, pesan teks, dokumen, gambar, suara dan video.

- d. Pembangunan sistem menggunakan bahasa pemrograman Java dan aplikasi pengembang yaitu Android Studio.
- e. Dijalankan pada sistem operasi android minimum SDK android Jellybean API 16.

#### **1.4 Tujuan Penelitian**

Tujuan dari penelitian ini adalah menghasilkan aplikasi pengamanan file dan pesan teks dengan teknik enkripsi dan dekripsi menggunakan AES 256 dan SHA 256 berbasis android untuk membantu pengguna dalam mengamankan file dan pesan teks pada perangkat sistem operasi berbasis android.

#### **1.5 Sistematika Penulisan**

Sistematika penulisan skripsi ini dilakukan secara bertahap dan disesuaikan dengan kebutuhan peneliti dalam penulisan, serta bertujuan agar skripsi ini dapat dipahami dengan jelas secara keseluruhan. Adapun sistematikanya adalah sebagai berikut :

##### **BAB 1 PENDAHULUAN**

Pendahuluan berisi tentang gambaran umum tentang masalah yang dibahas. Bab ini berisi tentang Latar belakang, Perumusan Permasalahan, Pembatasan Masalah, Tujuan Penelitian, Metode Penelitian dan Sistematika Penulisan.

##### **BAB 2 TINJAUAN PUSTAKA**

Memuat tinjauan dan ulasan singkat mengulas pentingnya penelitian dilakukan dan menyampaikan teori yang berhubungan dengan permasalahan yang dibahas sebagai dasar analisa permasalahan yang diteliti .

##### **BAB 3 METODE PENELITIAN**

Merupakan kerangka pendekatan studi dan dapat berupa analisis teori, metode eksperimen, kombinasi, rancangan, spesifikasi sistem baik hardware maupun software.

## BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi hasil keluaran dari sistem yang telah dibuat dan dibahas sesuai penelitian dan hipotesis untuk menjawab permasalahan yang ada.

## BAB 5 PENUTUP

Dalam bab ini memuat ringkasan hasil penelitian dan menjawab tujuan penelitian atau hipotesis. Bab ini juga memuat saran yang diungkapkan untuk mendapatkan hasil yang lebih baik terhadap sistem yang telah dibuat.

## DAFTAR PUSTAKA

## RIWAYAT HIDUP

## LAMPIRAN

