# BAB I

# PENDAHULUAN

Bab ini akan membahas mengenai pendahuluan. Pokok bahasan yang terdapat pada bab ini adalah latar belakang, perumusan masalah, batasan masalah, keaslian penelitian, manfaat penelitian, dan tujuan penelitian.

## 1.1. Latar Belakang

Berkomunikasi satu sama lain merupakan salah satu sifat dasar manusia sejak ada di muka bumi ini. Cara manusia berkomunikasi dari dulu sampai sekarang terus mengalami evolusi, yaitu dari model komunikasi tradisional bertransformasi menjadi model komunikasi komtemporer. Salah satu sarana komunikasi manusia adalah tulisan. Tulisan ini terdiri dari beberapa kata yang mengandung makna tertentu. Adanya tulisan ini bertujuan untuk menyampaikan maksud dari komunikator atau pengirim kepada komunikate atau penerima. Dunia semakin canggih dan teknologi informasi semakin berkembang. Seiring dengan berkembangnya era teknologi digital dan pertukaran data secara elektronis, keamanan informasi yang semula tidak begitu mendapat perhatian kini menjadi isu yang sangat penting sejak populernya teknologi *mobile (smartphone) communication* dan internet.

Perkembangan teknologi informasi yang sangat pesat ini, turut memajukan media komunikasi sebagai salah satu media penyampaian informasi dari suatu tempat ke tempat lainnya. Kemudahan pengaksesan media komunikasi oleh

semua orang, tentunya akan memberikan dampak bagi keamanan informasi atau bahaya pesan yang menggunakan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkan suatu metode yang dapat menjaga kerahasian informasi ini, yang salah satunya dikenal dengan sebutan kriptografi.

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* yang berarti *secret* (rahasia) dan *graphia* yang berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan informasi atau pesan ketika pesan tersebut dikirim dari satu tempat ke tempat lain. Berbicara pada ranah keamanan akan sebuah informasi yang melibatkan kriptografi tentunya tidak terlepas dengan algoritma.

Algoritma kriptografi dikelompokan mejadi dua kelompok yaitu algoritma simetris dan asimetris. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Sedangkan algoritma asimetris adalah kunci yang digunakan untuk proses enkripsi berbeda dengan kunci yang digunakan untuk proses dekripsi. Pada dasarnya algoritma simetris juga dikelompokan menjadi dua kategori yaitu blok kode dan aliran kode. Kinerja setiap algoritma berbeda dalam proses enkripsi maupun dekripsi sebuah data teks, sehingga apabila ketika melakukan proses enkrip maupun dekrip pada perangkat *mobile* seringkali terjadi *hang* karna mungkin spesifikasi perangkat *mobile* tidak mencukupi untuk melakukan proses tersebut.

*Android* hadir dengan begitu memanjakan pengguna akan fitur-fiturnya. Tentunya untuk mendukung fitur-fitur pada *android* yang begitu mulitifungsional membutuhkan sebuah perangkat *mobile* yang nantinya bisa mendukung kinerja fitur dari aplikasi itu sendiri, sehingga kinerjanya bisa dioptimalkan. Bila ditinjau dari kacamata bisnis, maka ini merupakan sebuah momentum kehadiran akan berbagai merek perangkat *mobile*. Dengan hadirnya berbagai macam merek *smartphone* dan spesifikasi yang berbeda-beda. Maka untuk mengetahui kinerja sebuah algoritma untuk proses enkripsi dan dekripsi yang nantinya berjalan pada salah satu merek *smartphone* tentunya menjadi dilema tersendiri untuk para pengembang aplikasi.

Realita yang ada menurut data yang dirilis *IDC (International Data Corporation)* april 2012 pengguna *smartphone* berbasis sistem operasi *android* di Indonesia mengalami peningkatan 28% dari tahun dari tahun lalu. Berdasarkan latar belakang yang ada penulis mencoba menganalisis dan membandingkan kinerja algoritma kriptografi *AES, DES* dan *IDEA* yang tepat digunakan untuk aplikasi proses enkripsi dan dekripsi data teks pada perangkat *mobile* sesuai dengan kapasitas spesifikasi perangkat *mobile* tersebut yang tentunya kinerja optimal yang diharapkan. Dengan demikian para pengembang aplikasi khususnya yang berbasis *android* tidak lagi rancuh dalam memilih algoritma.

## 1.2. Rumusan Masalah

Dengan adanya berbagai macam jenis algortima kriptografi, pemilihan akan algoritma sesuai dengan spesifikasi *platform smartphone* yang berkembang saat ini menjadi dilema pada pihak pengembang apllikasi. Berdasarkan latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah bagaimana merancang sebuah alat bantu atau aplikasi pembanding untuk analisis perbandingan algoritma kriptografi *AES, DES* dan *IDEA.*

## 1.3. Batasan Masalah

Agar pemebahasan tidak melebar dari topik, maka penulis membatasi permasalahan penelitian yaitu :

a. Aplikasi yang dirancang ini hanya digunakan sebagai alat bantu analisis algoritma kriptografi *AES, DES* dan *IDEA* untuk kepentingan penelitian, tidak digunakan secara umum untuk pengguna *smartphone* khususnya yang berbasis sistem operasi *android.*

b. Penelitian ini membandingkan kinerja tiga algoritma kriptografi yaitu *AES, DES* dan *IDEA* untuk proses enkripsi dan dekripsi *file* teks (.txt).

## 1.4. Keaslian Penelitian

Penelitian yang dibuat mengenai analisis perbandingan algoritma kriptografi *AES, DES* dan *IDEA* yang tepat untuk perangkat *mobile* belum pernah dilakukan oleh peneliti lain.

## 1.5. Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui kinerja dari algoritma *AES, DES* dan *IDEA* saat melakukan proses enkripsi maupun dekripsi *file* teks *(.txt)* pada salah satu perangkat *mobile* dengan spesifikasi terntentu.

Beberapa manfaat yang akan diperoleh dari penelitian ini adalah sebagai berikut :

a. Bagi Pihak Pengembang Aplikasi

   Memberikan kemudahan bagi Pihak Pengembang Aplikasi untuk mengevaluasi algoritma-algoritma kriptogarfi yang akan digunakan pada aplikasi enkripsi khususnya pada perangkat *mobile*.

b. Bagi Pembaca

   Dapat dijadikan bahan referensi di bidang penelitian kriptografi.