

# **BAB I**

## **PENDAHULUAN**

### **I.1 Latar Belakang**

Pada saat ini, keamanan informasi menjadi hal penting dalam penyimpanan dan transmisi data. Penggunaan data citra semakin luas dalam berbagai bidang. Oleh karena itu, pengamanan data citra dari akses yang tidak berhak menjadi hal yang penting. Untuk memenuhi aspek kerahasiaan pesan atau data lainnya dapat digunakan teknik kriptografi, dimana pesan yang dikirim hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut dengan menggunakan kunci rahasia.

Perkembangan ilmu pengetahuan saat ini telah mengalami kemajuan. Sama halnya dengan perkembangan teknologi, dimana teknologi saat ini telah banyak menghasilkan berbagai sumber aplikasi yang beragam jenis dan fungsinya salah satunya aplikasi dalam jenis transfer data atau *file*. Saat ini pemanfaatan aplikasi dalam pengiriman *file* sudah menjadi kebutuhan tersendiri bagi pihak umum untuk mengirim dan berbagi informasi. Namun masih seringnya kegiatan transfer data atau *file* yang dikirim terganggu atau diserang oleh pihak yang tidak bertanggung jawab. Untuk itu sangat pentingnya pengamanan file atau citra sehingga keamanan citra atau *file* yang dikirim dapat terjamin. Untuk meningkatkan kemanan transfer *file* dilakukan penerapan algoritma DES dan AES dalam pengamanan citra pada proses transfer data.

Dalam perancangan aplikasi yang direncanakan memungkinkan pengiriman citra menjadi lebih cepat karena pengiriman dapat dilakukan di berbagai tempat dengan pemanfaatan Android. Penerapan algoritma DES menggunakan pengkodean yang sama dan AES menggunakan pengkodean yang berbeda menjadikan *file* citra yang dikirim terjamin keamanannya. Dengan itu, berdasarkan latar belakang diatas maka penulis tertarik untuk mengangkat penulisan skripsi ini dengan judul "**Perancangan Pengamanan Citra Pada Proses Transfer File Menggunakan Algoritma DES dan AES Berbasis Android**".

## **II.1 Ruang Lingkup Permasalahan**

### **II.1 Identifikasi Masalah**

Adapun permasalahan yang penulis rangkum dalam penelitian dan perancangan adalah:

1. Masih seringnya kecurangan atau pembobolan file terkirim yang dilakukan oleh pihak yang tidak bertanggung jawab.
2. Masih berkurangnya suatu sistem aplikasi pengamanan citra dalam transfer data dengan penerapan algoritma DES dan AES pada perangkat *android*.
3. Dibutuhkannya suatu aplikasi pengamanan citra yang dengan mudah dipahami oleh pengguna.

### **II.2 Perumusan Masalah**

Berdasarkan identifikasi masalah yang telah penulis rangkum, maka dihasilkan rumusan masalah sebagai berikut :

1. Bagaimana perancangan suatu aplikasi pengamanan citra pada proses transfer data menggunakan algoritma DES dan AES?
2. Bagaimana tingkat keamanan yang ada pada penerapan algoritma DES dan AES untuk pengamanan citra pada transfer data berbasis *android*?

### **II.3 Batasan Masalah**

Dalam proses perancangan terhadap aplikasi ini, penulis membatas permasalahan yang akan dibahas, diantaranya adalah :

1. Dalam perancangan hanya berfokus pada pengamanan data citra.
2. Perancangan pengamanan data citra hanya sebatas penerapan algoritma DES dan AES.
3. Pengembangan menggunakan pemrograman *Visual Basic*, *VB.Net* sebagai mesin pemrograman.

### **III.1 Tujuan Dan Manfaat**

#### **III.1 Tujuan Penelitian**

Adapun tujuan dari penelitian ini adalah :

1. Untuk menyediakan aplikasi pengamanan citra berbasis *android*.
2. Untuk mengimplementasikan keamanan data dengan penerapan algoritma DES dan AES.
3. Untuk menambah wawasan penulis dalam merancang aplikasi pengamanan citra dalam transfer data yang berbasis *android*.

### **III.2 Manfaat Penelitian**

Adapun beberapa manfaat dari penelitian ini adalah sebagai berikut:

1. Diharapkan memberikan keamanan dalam pengiriman data citra yang dengan mudah digunakan oleh user atau pengguna.
2. Menghindari manipulasi atau penerobosan oleh pihak-pihak yang tidak bertanggung jawab dalam pengiriman citra yang berbasis *android*.

### **IV.1 Metodologi Penelitian**

Metode yang digunakan dalam melaksanakan penelitian serta menyelesaikan masalah adalah :

1. Metode Penelitian Kepustakaan (*Library Research*).

Penulis melakukan studi pustaka untuk memperoleh data-data yang berhubungan dengan penulisan Skripsi dari berbagai sumber bacaan seperti : buku Bahasa Pemograman *Java*, Enkripsi, algoritma *DES* dan lain sebagainya.

2. Studi kepustakaan (*Dictionary Reserach*)

Dalam penulisan skripsi ini, penulis melakukan studi kepustakaan mencari beberapa buku, jurnal, dan yang lainnya untuk mencari yang berhubungan dengan pengamanan citra, *java*. Dan sumber lainnya yang berhubungan dengan permasalahan dalam penulisan skripsi ini.

3. Analisis Kebutuhan

Dalam analisis kebutuhan penulis memerlukan data aplikasi perancangan enkripsi *file*.

#### 4. Spesifikasi dan Desain.

Sistem yang akan penulis buat nantinya akan diuji coba menggunakan software dan hardware, antara lain sebagai berikut :

- a. *Software* yang digunakan sistem operasi *Microsoft Windows Seven, SDK Java*.
- b. *Hardware*, Processor CoreDuo 1,8 Ghz, Ram 2 GB, Hardisk 80 GB, Vga, Nvidia 210GT 1 Gb, LCD 17”, Keyboard + Mouse
- c. Uji Coba Proses uji coba terhadap aplikasi yang telah selesai dirancang dilakukan dengan memasukan *input* data kedalam aplikasi untuk kemudian dijalankan.
- d. Validasi, Pada proses akhir dari keseluruhan adalah validasi, aplikasi hasil perancangan akan dinyatakan valid atau sesuai apabila seluruh proses data sesuai dengan perancangan.

#### V.1 Keaslian Penelitian

Pada setiap penelitian yang dilakukan memiliki bukti keaslian, dimana penelitian-penelitian terdahulu memiliki bukti tersendiri. Dengan itu untuk lebih jelasnya keaslian-keaslian tersebut dapat dilihat pada tabel 1 sebagai berikut.

**Tabel I.1. Keaslian Penelitian**

No	Peneliti	Judul	Hasil
1	Gede Andika Putra, Made Widhi Wirawan (2012)	Sistem pengamanan data sidik jari menggunakan algoritma aes pada Sistem kependudukan berbasis <i>radio frequency identification</i> (RFID)	pengujian RMS yang telah dilakukan data sidik jari yang diamankan dalam tag RFID tidak dapat digunakan oleh penduduk yang tidak berhak.
2	Mandeep Singh Narula(2014)	Implementation of Triple Data Encryption Standard using Verilog	menerapkan algoritma DES dan Triple DES menggunakan tingkat tinggi Verilog bahasa deskripsi hardware . Ini adalah solusi yang fleksibel untuk sistem dan keamanan lapisan kriptografi protokol nirkabel . Industri pembayaran elektronik menggunakan Triple DES dan terus mengembangkan dan menyebarluaskan standar berdasarkan itu untuk melindungi konten pengguna dan data sistem .

## VI.1 Sistematika Penulisan

Susunan dan sistematika penulisan Skripsi ini terdiri dari beberapa sub bab dapat dilihat sebagai berikut.

### BAB I : PENDAHULUAN

Pada bab ini secara ringkas diterangkan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penyelesaian masalah, serta sistematika penulisan.

## **BAB II : TINJAUAN PUSTAKA**

Sub bab ini tentang teori yang berkaitan dengan pembuatan, desain dan tampilan perancangan aplikasi pengamanan cirta dengan menggunakan Algoritma DES, serta teori-teori yang mendukung analisa penelitian.

## **BAB III : ANALISA DAN PERANCANGAN PROGRAM**

Berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, *Java* serta ketentuan penggunaan.

## **BAB IV : HASIL DAN PEMBAHASAN**

Berisi tentang tampilan hasil implemtasi program, beserta pembahasannya, serta kelebihan dan kekurangan sistem yang dirancang.

## **BAB V : KESIMPULAN DAN SARAN**

Dalam bab ini diuraikan kesimpulan dan saran yang dapat diberikan untuk pengembangan aplikasi yang dirancang.