BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem keamanan data dipasang untuk mencegah pencurian, kerusakan dan penyalahgunaan data yang disimpan melalui smartphone. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran public. Teknologi jaringan komputer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik, namun gangguan tetap bias terjadi karena ada unsur kesengajaan yang mengarah ke penyalahgunaan system dari pihak-pihak tertentu.

Kriptografi adalah ilmu sekaligus seni yang dimanfaatkan untuk menjaga keamanan pesan (Schneier, 1996). Pengamanan ini dilakukan dengan menggunak an metode enkripsi dan dekripsi dengan menggunakan kunci khusus. Pesan yang belum mengalami proses enkripsi disebut *plaintext*, sedangkan pesan yang telah mengalami proses enkripsi disebut *chiphertext*. Akan tetapi jika objek yang dienkripsi berupa citra digital disebut dengan *plain image* dan *chiperimage*. Ada banyak algoritma yang dapat digunakan untuk menjaga keamanan citra digital seperti *Rijndael, Serpent, Twofish,MARS, RC6, MRC6, RSA* (Rivest, Shamir, Adleman), dan lain-lain. Enkripsi adalah salah satu teknik yang paling baik untuk menjaga kerahasiaan suatu data dalam berkomunikasi. Dengan enkripsi, suatu informasi akan menjadi sulit untuk diketahui oleh orang yang tidak berhak.

DES (Data Encryption Standard) merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Algoritma DES (Data Encryption Standard) merupakan modifikasi daripada algoritma terdahulu yang bernama *Lucifer*. *Lucifer* merupakan algoritma *cipher block* yang beroperasi pada blok masukkan 64 bit dan kuncinya berukuran 128 bit. Pengurangan jumlah bit kunci pada DES dilakukan dengan alasan agar mekanisme algoritma ini biasa di implementasikan dalam satu chip.

Meskipun DES merupakan algoritma yang sudah banyak digunakan, ternyata algoritma ini dianggap belum memiliki tingkat keamanan yang cukup. Karena itulah, untuk meningkatkan keamanannya dilakukan beberapa cara. Cara yang pertama adalah mengubah susunan S-Box nya sedemikian rupa, sehingga distribusinya lebih merata. Sedangkan cara yang kedua adalah dengan menggunakan teknik DES yang diulang seperti *Double* DES dan *Triple* DES. Teknik *Differential Cryptanalysis* merupakan sebuah teknik yang sangat banyak digunakan untuk memecahkan berbagai algoritma enkripsi blok berbasiskan permutasi dan substitusi. Beberapa algoritma enkripsi blok lain juga yang lemah terhadap serangan ini misalnya adalah algoritma FEAL, REDOC-II and LOKI. Meskipun demikian, apabila jumlah ronde pada DES dinaikkan, maka teknik ini sudah tidak terlalu ampuh lagi, meskipun masih lebih baik daripada teknik *brute force.*

Dengan alasan tersebut, NIST mengadakan sayembara terbuka untuk membuat standard algoritma kriptografi yang baru sebagai pengganti DES. Standard tersebut kelak diberi nama *Advanced Encryption Standard* (AES). Persyaratan yang diajukan oleh NIST tentang algoritma yang baru tersebut adalah:

1. Algoritma yang ditawarkan termasuk ke dalam kelompok algoritma kriptografi simetri berbasis *cipher* blok.
2. Seluruh rancangan algoritma harus publik (tidak dirahasiakan).
3. Panjang kunci fleksibel: 128, 192, dan 256 bit.
4. Ukuran blok yang di enkripsi adalah 128 bit.
5. Algoritma dapat diimplementasikan baik sebagai *software* maupun *hardware*.

NIST menerima 15 proposal algoritma yang masuk. Konferensi umum pun diselenggarakan untuk menilai keamanan algoritma yang diusulkan. Pada bulan Agustus 1998, NIST memilih 5 finalis yang didasarkan pada aspek keamanan algoritma, kemangkusan (*efficiency*), fleksibilitas, dan kebutuhan memori (penting untuk *embedded system*). Finalis tersebut adalah:

1. *Rijndael* (dari Vincent **Rij**men a**n**d Joan **Dae**men – Be**l**gia, 86 suara)

2. *Serpent* (dari Ross Anderson, Eli Biham, dan Lars Knudsen – Inggris, Israel, dan Norwegia, 59 suara).
3. *Twofish*(dari tim yang diketuai oleh Bruce Schneier – USA, 31 suara).
4. *RC6* (dari Laboratorium *RSA* – USA, 23 suara).
5. *MARS* (dari IBM, 13 suara)

Pada bulan Oktober 2000, NIST mengumumkan untuk memilih Rijndael (dibaca: Rhine-doll), dan pada bulan November 2001, Rijndael ditetapkan sebagai AES, dan diharapkan Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun. Rijndael adalah salah satu algoritma enkripsi simetris. Dimana proses enkripsi dan dekripsinya menggunakan kunci yang sama. *Rijndael* merupakan algoritma yang ditetapkan sebagai standar metode enkripsi modern pengganti DES (*Data Encryption Standard*), dalam sayembara AES (*Advanced Encryption Standard*) oleh NIST(*National Institute of Standards and Technology)*

Dirancang untuk menggantikan DES (launching akhir 2001), menggunakan variable length block chipper, key length: 128 bit, 192-bit, 256-bit, dapat diterapkan untuk smart card. Algoritma Rijndael yang ditetapkan sebagai AES memiliki karakteristik yang istimewa yang menjadikannya mendapat status tersebut. Dalam hal ini pula maka algoritma ini perlu untuk dipelajari karena penggunaannya di kehidupan sehari-hari sudah sangatlah banyak dan hal ini akan berguna dalam pengembangan dari teknologi kriptografi agar dapat menemukan terobosan-terobosan baru. Tujuan utama dari kriptografi adalah melindungi sebuah informasi, begitu pula dengan AES yang dengan serangkaian tahap atau ronde yang dilakukan dengan menggunakan kunci simetris. Penggunaan AES pun bukan hanya digunakan dalam hal sederhana melainkan perannya sangatlah krusial dalam sebuah perangkat lunak ataupun dalam hal ini dimana AES tersebut digunakan.

Pada saat ini, umumnya masyarakat sudah mulai menyukai system operasi *smartphone* berbasis *Android* dibandingkan system operasi lainnya. Hal tersebut dibuktikan dengan persentase penggunaan akhir *Android* mencapai 86,2% pangsa pasar diseluruh dunia (Market Share, 2016).

Berdasarkan uraian di atas, pembuatan aplikasi ini diberikan judul "Aplikasi Keamanan Gambar dengan Kriptografi Menggunakan Algoritma AES (Advanced Encryption Standard)". Aplikasi ini berguna untuk pengaman citra digital pada *smartphone Android*.

1.2 Perumusan Masalah

Adapun rumusan masalah berdasarkan uraian sebelumnya adalah bagaimana cara mengamankan suatu gambar dengan kriptografi menggunakan algoritma AES (Advanced Encryption Standard).

1.3 Pembatasan Masalah

Dalam pembuatan aplikasi ini ruang lingkup atau batasan masalah yang diuraikan sebagai berikut :

1. Dalam pembuatan aplikasi ini menggunakan *Platform Android* dengan minimum *operation system Jelly Bean*4.1.
2. Objek yang digunakan berupa citra digital dengan format file jpg.
3. Algoritma kriptografi yang dipakai dalam aplikasi ini adalah algoritma AES dengan panjang kunci 128 bit.
4. Ukuran gambar yang digunakan adalah 300 x 300 piksel.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan utama yang ingin dicapai dari pembuatan aplikasi ini adalah mengetahui cara pengamanan gambar dengan kriptografi menggunakan algoritma AES (Advanced Encryption Standard).

1.4.2 Manfaat

Adapun manfaat dari pembuatan aplikasi ini adalah sebagai berikut :

1. Mengetahui ilmu tentang kriptografi.
2. Mendapatkan gambar yang aman setelah proses enkripsi.

1.5 Metodologi Penulisan

Untuk mempermudah penulisan dalam peyusunan laporan akhir maka penulis menggunakan metode-metode sebagai berikut:

1. Metode Studi Pustaka

   Dengan metode ini penulis mempelajari buku-buku yang berhubungan dengan masalah yang akan dibahas sebagai referensi.

2. Metode Eksperimen

   Yaitu tahap pembuatan aplikasi dengan cara memprogram menggunakan Android Studio.

3. Metode Observasi

   Yaitu merupakan metode pengamatan simulasi dengan mencoba memasukkan gambar agar dapat di enkripsi dan dekripsi dengan algoritma AES (Advanced Encryption Standard) dalam bentuk aplikasi yang dijalankan oleh program android.

4. Metode Wawancara

   Metode ini dilakukan penulis dengan melakukan tanya jawab dengan dosen pembimbing, dosen pengajar, dan rekan-rekan mahasiswa.

1.6 Sistematika Penulisan

Untuk memudahkan penulisan, maka dalam sistem penulisan laporan akhir ini penulis membaginya dalam lima bab yang tersusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang permasalahan, permasalahan dan pembatasan masalah, tujuan dan manfaat, metodologi penulisan, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tentang landasan teori yang mendukung dalam pembuatan laporan akhir.

BAB III RANCANG SISTEM APLIKASI

Mengenai teori-teori yang akan digunakan untuk pemecahan masalah pada pembahasan, serta data-data yang didapat pada saat pembuatan aplikasi.

BAB IV PEMBAHASAN

Pada bab ini membahas tentang analisa dan hasil yang didapat pada saat enkripsi dan dekripsi.

BAB V PENUTUP

Bab ini berisi kesimpulan yang diambil dari pembuatan aplikasi serta saran-saran yang mungkin berguna untuk pengembangan aplikasi tersebut.