BAB I

PENDAHULUAN

1.1. Latar Belakang

Citra Digital sering digunakan dalam menyajikan berbagai informasi didalamnya, citra digital dapat menjadi hal yang penting apabila citra digital tersebut memiliki informasi yang berharga, dan dapat menjadi bersifat pribadi, karena pada dasarnya data informasi berupa citra digital sangat dibutuhkan dibandingkan dari data yang sifatnya teks dan digunakan dalam berbagai bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Penggunaan teknik digital bagi transmisi dan penyimpanan citra digital, masalah mendasar untuk melindungi kerahasiaan, keutuhan dan keaslian citra digital memang perlu diperhatikan. Kerahasiaan suatu informasi sangatlah penting dan bersifat pribadi, karena pencurian data, dan serangan terhadap data berupa citra digital yang secara langsung ataupun tidak langsung dapat menimbulkan berbagai permasalahan yang dapat menimbulkan dampak serius terhadap permasalahan ilegal, sosial, dan ekonomi, karena tidak semua informasi yang ada dibuat untuk konsumsi secara umum. Kasus yang sering terjadi adalah rekayasa foto atau pun penyebaran foto secara ilegal tentunya hal ini merugikan pemiliknya, sehingga diperlukan suatu pengamanan dari sumber-sumber yang berkepentingan tentunya yang menghasilkan suatu produk berupa citra digital (Ibrahim, 2012).

Contoh kasus pencurian foto pribadi terjadi pada Akhir 2014 lalu, peredaran foto pribadi beberapa artis Hollywood sempat membuat geger jagat

maya. Para artis, antara lain Jennifer Lawrence, Lea Michele, dan Kirsten Dunst, ternyata menjadi korban peretasan akun *iCloud* oleh *hacker* yang mencuri foto-foto pribadi mereka. Setelah hampir dua tahun, pria yang diduga sebagai dalang pencurian foto tak senonoh tersebut akhirnya mengaku bersalah atas tindak peretasan yang dituduhkan, sebagaimana dilaporkan *Buzzfeed* dan dihimpun KompasTekno, Rabu (16/3/2016). Ryan Collins, peretas berumur 36 tahun yang telah menghimpun foto bugil para artis dalam periode dua tahun, terhitung sejak 2012 hingga 2014. Pengakuan Collins diumbar Departemen Kehakiman Amerika Serikat. Jaksa penuntut menjelaskan, Collins menggunakan trik mengelabui target dengan mengirim sebuah e-mail yang didesain khusus agar seakan-akan tampak berasal dari *Apple* atau *Google (phising)*. E-mail itu berisi permintaan mengisi *username* dan *password*. Target atau korban diharap mau membalas dan memberikan informasi yang diminta. Sekali saja target merespons, Collins sudah bisa mengakses semua informasi personal sang target. Collins juga menggunakan sebuah program di komputer untuk mengunduh semua konten dari akun *iCloud* korbannya. Menurut dokumen pengadilan, Collins telah mengakses 50 akun *iCloud* dan 72 akun Gmail. Meski mengaku mencuri foto personal para artis, Collins enggan dituduh menyebar foto tersebut ke jagat maya via forum *online* Reddit dan 4chan. Dokumen yang dihimpun jaksa penuntut, memang belum ada bukti kuat yang membenarkan dugaan tersebut (Bohang, 2016).

Mengamankan data berupa citra digital dapat menggunakan teknik kriptografi, Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian

ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES/Rijndael sendiri adalah algoritma kriptografi dengan menggunakan algoritma AES/Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit (Ibrahim, 2012).

Transformasi Base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary*. Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari A….Z, a….z dan 0….9, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu buah karakter sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan. Kriptografi transformasi Base64 banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data, ini dikarenakan

hasil dari Base64 berupa *plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary (Nugroho, 2015).

1.2. Rumusan Masalah

Berdasarkan dari latar belakang masalah, maka permasalahan yang didapat adalah:

Bagaimana menerapkan *Encoder* BASE64 dan Algoritma AES pada aplikasi enkripsi dan dekripsi sebagai sarana pengamanan gambar.?

1.3. Batasan Masalah

1. Ukuran Gambar yang dapat digunakan pada proses enkripsi maksimal 10MB
2. Ukuran file hasil enkripsi yang dapat didekripsi maksimal 20MB
3. Gambar yang dapat diproses berupa gambar bertipe .jpg

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah :

Membuat Aplikasi enkripsi dan dekripsi gambar menggunakan *Encode* Base64 dan Algoritma AES.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah membantu bagi pengguna yang menggunakan aplikasi ini dalam mengamankan file berbentuk gambar yang bersifat rahasia agar tidak disalah gunakan oleh pihak yang tidak berhak. Aplikasi ini juga membutuhkan kunci rahasia untuk mengembalikan file hasil enkripsi kebentuk semula

1.6. Metodologi Penelitian

Langkah-langkah yang perlu dilakukan untuk meralisasikan aplikasi yang akan dibuat adalah sebagai berikut:

1. Pemahaman Sistem dan Studi Literatur

   Penulis menggunakan buku dan jurnal baik yang berupa tulisan maupun elektronik yang membahas tentang konsep-konsep yang berkaitan dengan penelitian.

2. Perancangan

3. Implementasi dan Pembangunan.

   Pada tahap ini sistem akan dibangun sebuah aplikasi enkripsi dan dekripsi citra digital menggunakan algoritma AES dan *Encode* Base64.

4. Pengujian aplikasi

   Pada tahap ini menguji coba aplikasi dengan menggunakan skenario yang sudah disiapkan, uji coba dan evaluasi perangkat dilakukan untuk mencari masalah yang mungkin timbul, mencari jalannya program, dan mengadakan perbaikan jika ada kekurangan.

5. Dokumentasi

   Proses dokumtasi hasil penelitian dilakukan selama penelitian dengan menyusun laporan dalam bentuk skripsi.

1.7. Sistematika Penulisan

Sistematika penulisan dibuat untuk lebih memperjelas alur sehingga dapat lebih mudah memahami materi. Laporan tugas akhir ini dibagi menjadi lima bab yang dilengkapi dengan penjelasan pada setiap bab, yaitu sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, yang menjadi dasar dibuatnya penelitian, identifikasi masalah yang berisi mengenai latar belakang masalah yang ditemukan, rumusan masalah mengenai permasalahan yang terjadi, batasan masalah, tujuan penelitian sebagai hasil dari langkah penyelesaian masalah, manfaat penelitian, metodologi penelitian sebagai langkah atau cara menyelesaikan masalah dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang berhubungan dengan penelitian Tugas Akhir sebagai penunjang landasan atau acuan penelitian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan garis besar perancangan perangkat lunak yang dilibatkan dalam perancangan aplikasi.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan pengujian aplikasi beserta analisa kinerja dengan menggunakan beberapa contoh file.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan yang merupakan jawaban dari tujuan penelitian. Saran yakni mengenai keterbatasan-keterbatasan yang ada dalam sistem yang dibuat.