BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Personal computer (*PC*) dan laptop saat ini sudah menjadi barang umum yang digunakan oleh masyarakat. Berkat kecanggihan teknologi, komputer menjadi alat yang sangat membantu berbagai macam kegiatan masyarakat. Tidak hanya itu, kemudahan komputer *portable* atau laptop membuat mobilitas mayarakat menjadi lebih mudah, semua kegiatan yang memiliki tingkat kesulitan yang tinggi ataupun tingkat kesulitan yang rendah dapat dikerjakan oleh komputer. Selain itu komputer juga sangat mudah dioperasikan, hal ini membuat komputer sangat mudah diterima di berbagai golongan umur di dalam mayarakat. Komputer itu sendiri membantu dalam membuat *file* atau data, menyimpan *file*, membagikan *file*, menghapus *file*, hingga menampilkan *file*. *File* tersebut terbagi kedalam beberapa jenis, mulai dari *file video, file photo* atau *image, file audio,* ataupun *file text.*

File yang disimpan di dalam komputer tersebut ada yang bersifat pribadi, sensitif, rahasia, hingga *file* yang bernilai tinggi. Tidak sembarang orang dapat melihat dan mengakses *file – file* tersebut. Karena sifat – sifat *file* diatas itulah, banyak sekali masalah – masalah atau pelanggaran – pelanggaran yang sering terjadi berkaitan dengan *file* komputer. Pelanggaran privasi adalah salah satu masalah yang menurut penulis sering terjadi. Orang lain melihat, mengubah, menambah, atau menghapus *file* yang bersifat sensitif, rahasia, hingga *file* yang

bernilai tinggi tanpa sepengetahuan dan seizin pemilik *file* tersebut. Pelanggaran privasi ini membuat pemilik *file* menjadi tidak nyaman dan merasa terganggu.

Akibat dari pelanggaran privasi ini, kerahasiaan suatu *file* menjadi rusak. Jika orang lain berhasil mengakses dan memodifikasi *file* tersebut dapat menimbulkan kerugian kepada pemilik *file*, baik dari segi materil dan non materil. Selain itu juga, dampak lain yang ditimbulkan adalah integritas *file* hilang atau rusak, karena *file* sudah mengalami perubahan. Hal – hal tersebut terjadi karena orang lain berhasil mengakses *file* tanpa sepengetahuan pemilik *file*.

Untuk menghindari masalah – masalah diatas, pemilik harus bisa menjaga kerahasiaan *file* tersebut. Banyak cara yang dapat digunakan, mulai dari penggunaan password hingga menentukan hak akses user didalam komputer. Selain kedua cara tersebut, cara lain yang lebih *advanced* adalah kriptografi. Kriptografi adalah ilmu yang mempelajari tentang penyandian data [1]. Kriptografi dapat diaplikasikan kedalam komputer menggunakan algoritma kriptografi yang sesuai. Algoritma kriptografi yang digunakan adalah *Advanced Encryption Standard (AES)* dan *Caesar Cipher Modivicatioan.* AES (*Advanced Encryption Standard*) adalah algoritma *symmetric block cipher* yang dapat melakukan enkripsi (*encrypt*) dan dekripsi (*decrypt*) informasi. Seperti yang dinyatakan oleh *Federal Information Processing Standards Publication* (FIPS) " The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data " [4]. Mengutip isi jurnal *IOSR Journal of Computer Engineering (IOSR-JCE) Caesar cipher* adalah algoritma yang sudah dikenal dengan luas, algoritma tipe substitusi ini bekerja dengan menukar huruf di dalam

plaintext dengan huruf lain yang memiliki selisih posisi tertentu di dalam alfabet [5]. Kedua algoritma kriptografi inilah yang akan di implementasikan ke dalam program yang akan dibuat.

Berdasarkan latar belakang yang telah dijabarkan di atas, maka penulis mengangkat skripsi dengan judul **" *Implementasi Kriptografi pada File Photo dan Video dengan menggunakan Algoritma AES dan Modifikasi Caesar Cipher pada Private Komputer* "**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana Implementasi Kriptografi pada File Photo dan Video dengan menggunakan Algoritma AES dan Modifikasi Caesar Cipher pada Private Komputer ?.

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan penulis dalam penelitian ini adalah sebagai berikut.

1. Modifikasi *Caesar Cipher* dalam judul memiliki arti dilakukan perubahan perubahan – perubahan yang diperlukan pada algoritma *Caesar Cipher.*
2. *Private computer* dalam judul memiliki arti komputer milik pribadi, komputer tersebut dapat berupa *personal computer (pc)* atau laptop.
3. Foto dan video *file* dalam judul memiliki arti data yang akan diolah atau digunakan oleh program hanya sebatas pada data foto dan data video.

4. *File* foto yang digunakan memiliki ekstensi *file* .jpg dan .png.

5. *File* video yang digunakan memiliki ekstensi *file* .mkv dan .mp4.

6. Sistem operasi yang digunakan adalah *Windows Operating System* dengan contoh kasus *Windows 10.*

7. Aplikasi dibuat menggunakan bahasa pemrograman C#.

1.4 Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini dimaksudkan untuk menganalisa, mendesain, dan mengimplementasikan algoritma *Advanced Encryption Standard* (AES) dan *Caesar Cipher* pada program di sistem operasi *Windows* sehingga program dapat memiliki kemampuan.

1. Menjalankan proses enkripsi (encrypt) *file*.
2. Menjalankan proses dekripsi (*decrypt*) *file*.
3. Meningkatkan kerahasiaan *file* foto dan video.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat bermanfaat untuk menjaga kerahasiaan *file* foto dan video pada *personal computer* yang menggunakan sistem operasi *windows*. Manfaat lain penelitian ini juga diharapkan dapat mengurangi rasa khawatir pengguna akan ancaman – ancaman terhadap *file* tersebut.

1.6 Metode Penelitian

Penulis melakukan beberapa metode penelitian dan juga melakukan pengumpulan data untuk memperoleh informasi – informasi yang diperlukan untuk memperoleh jawaban atas permasalahan yang penulis ungkapkan. Adapun metode – metode yang penulis lakukan adalah sebagai berikut.

1.6.1 Metode Pengumpulan Data

Metode pengumpulan informasi dan data yang digunakan dalam penelitian ini diantaranya :

1.6.1.1 Metode Observasi

Penulis melakukan pengamatan terhadap masalah yang diangkat. Pengamatan yang dilakukan berupa pencarian informasi – informasi yang dapat membantu penulis untuk mencari jawaban atas masalah yang ada. Informasi tersebut dapat diperoleh dari pengalaman penulis, pengalaman orang lain atau melalui tulisan – tulisan yang memiliki tema masalah yang sama dengn penulis.

1.6.1.2 Metode Studi Kepustakaan

Untuk mendukung perancangan program ini, penulis menggunakan studi kepustakaan sebagai referensi. Pustaka yang digunakan antara lain *journal, website, e-book,* buku atau penelitian – penelitian lain yang berkaitan dengan penelitian ini.

1.6.1.3 Metode Internet

Menggunakan metode *browsing* untuk mengumpulkan rujukan yang bersumber dari internet dengan mengunjungi situs yang berhubungan dengan

penelitian, mendownload *journal*, mendownload *e-book*, gambar – gambar, atau *tools* yang dapat digunakan dalam penelitian ini.

1.6.2 Metode Analisis

Berikut ini adalah metode analisis yang digunakan penulis dalam penyusunan tulisan ini adalah analisis kebutuhan sistem dan analisis kelayakan sistem.

1.6.2.1 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem adalah beberapa kebutuhan dalam sistem untuk mendukung jalannya proses pembuatan dan kinerja program yang dibuat.

1.6.2.2 Analisis Kelayakan Sistem

Analisis kelayakan sistem adalah untuk menentukan layak tidaknya program yang akan dibuat. Analisis ini menyangkut segi teknologi, operasional, hukum, dan ekonomi.

1.6.3 Metode Perancangan

Metode perancangan menggunakan perancangan UML (*Unified Modelling Language*).

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan penulis dalam penulisan skripsi ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang teori – teori dan tinjauan pustaka yang digunakan.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang analisis sistem, analisis kebutuhan, analisis kelayakan sistem, dan perancangan program.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang hasil program yang yang sudah dibuat. Membahas kode – kode program yang digunakan serta hasil anlisa yang didapatkan.

BAB V PENUTUP

Bab ini membahas tentang kesimpulan dari keseluruhan laporan dan saran yang membangun untuk menambah kesempurnaan program.