BAB I

PENDAHULUAN

1.1 Latar Belakang

Maraknya perkembangan teknologi di zaman serba digital sekarang ini sangatlah menunjang kegiatan manusia, terutama dibidang inovasi dan kretifitas dalam bekerja, belajar, penyebaran informasi dan lain lain. Sayangnya semakin maju teknologi di zaman modern ini, semakin maju pula tingkat kejahatan dengan teknologi sekarang. Oleh karena itu edukasi terhadap penggunaan teknologi sangat diperlukan, pengamanan data yang tepat diperlukan guna meningkatkan keamanan yang menjamin agar tidak disalah gunakan oleh orang yang tak bertanggung jawab untuk keperluan yang tidak semestinya. Banyaknya jenis kejahatan dimasa sekarang perlu diwaspadai, salah satunya *cyber crime*. *Cyber Crime* dapat diartikan sebagai tindak kenjahatan di dunia maya yang menjadikan teknologi komputer dan jaringan internet sebagai sasarannya.

Data yang bersifat pribadi menjadi objek yang disenangi oleh *hacker* untuk dimanupulasi, dipermaikan dan digunakan tidak pada semestinya. Oleh karena itu data yang bersifat pribadi atau rahasia perlu dijaga keamanannya. Ada beberapa teknik pengamanan data, diantaranya adalah teknik enkripsi. Enkripsi merupakan sebuah proses pengubahan sebuah pesan atau informasi dari yang bisa dimengerti atau dibaca menjadi sebuah pesan atau informasi yang sulit dimengerti hingga tidak terbaca sama sekali.Teknik enkripsi dapat mengamankan data karena data dapat berubah menjadi tidak terbaca sesuai dengan aslinya. Dan data yang terenkripsi dapat terbaca lagi apabila sudah di deskripsi dengan menggunakan kunci yang tepat. Dan dengan mengenkripsi data file yang penting atau rahasia dapat meningkatkan keamanan data yang bersifat rahasia tersebut.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data (Ratno Prasetyo, 2016). Dalam ilmu kriptografi terdapat dua proses penyandian yang disebut enkripsi dan deskripsi. Enkripsi dilakukan pada proses pengiriman pesan atau informasi dengan cara mengubah data asli kedalam bentuk kode kode yang menjadikannya data rahasia sedangkan deskripsi dilakukan pada

proses penerimaan dengan cara mengubah data yang berisi kode kode rahasia tersebut ke dalam bentuk data yang asli dan mudah dimengerti.

Pada tanggal 27 Desember 2020 berita tentang kebocoran data sensitif dari artis kenamaan ibu kota yang meramaikan *headline* berita di televisi dan *online*. Maka dari itu diperlukannya enkripsi file untuk file yang dianggap penting oleh user. Oleh karena itu universitas Bhayangkara Jakarta Raya sebagai perguruan tinggi swasta yang terletak di kota Bekasi, Jawa Barat. Pada Universitas Bhayangkara Jakarta Raya mempunyai banyak data file penting yang bersifat rahasia suatu lembaga, seperti data data keuangan dan data penting lainnya pada komputer atau laptop di lembaga mereka. Dan apabila data tersebut bisa saja dicuri dan dimanipulasi pada suatu kejadian yang dapat merugikan lembaga. Data keuangan yang tidak terenkripsi atau tidak dirahasiakan dapat dengan sangat mudah dimanipulasi oleh orang yang tidak bertanggung jawab untuk mengambil keuntungan di lembaga yang bergerak dibidang pendidikan tersebut, seperti dikorupsi pada jumlah pengeluaran untuk biaya operasional perusahaan tersebut dan biaya biaya lainnya dan apabila data data tersebut di hack oleh virus yang terjangkit di dalam computer seperti data keuangan dan data penting lainnya maka data tersebut akan terenkrip dengan virus dan tidak bisa dikembalikan lagi datanya. Oleh karena itu penulis berniat untuk menjadikan hal tersebut sebagai bahan penelitian penulis guna menyelesaikan tugas akhir untuk jenjang strata satu yang penulis tempuh. Dengan mengamankan data data rahasia lembaga pendidikan Universitas Bhyangkara Jakarta Raya menggunakan teknik enkripsi dan dekripsi yang penulis terapkan pada penelitian ini semoga dapat membantu lembaga tersebut untuk dapat menjaga kerahasiaan data mereka. Oleh karena itu, terdapat metode algoritma kriptografi yang cocok untuk memecahkan masalah pengamaanan data lembaga tersebut, yaitu salah satunya adalah metode AES dan SHA. Advanced Encryption Standar (AES) adalah algoritma kriptografi simetris modern yang beroperasi dalam mode penyandian blok (block cipher) yang memproses blok data dengan ukuran 128-bit dengan panjang kunci 128-bit, 192-bit, atau 256-bit (Asep Suryana, 2016). Terdapat beberapa mode dalam algoritma AES diantaranya mode CBC, ECB, OFB, CTR dan CFB untuk penyadian dengan metode *block cipher*. Penulis menggunakan mode CBC atau yang sering disebut *Cipher Block Chaining*

ialah metode penyandian blok berulang seperti rantai yang menggunakan veckor inisialisasi (IV) atau sering disebut deret biner unik dengan panjang tertentu untuk tiap enkripsi. Salah satu karakteristik utamanya CBC menggunakan mekanisme rantai yang membuat *chipertext* blok sebelumnya bergantung pada semua blok *chipertext* sebelumnya. Dengan segala pertimbangan mode operasi AES yang ada, penulis memilih untuk menggunakan mode CBC dengan segala kelebihan dan kekuranganya. SHA merupakan algoritma *Hashing* atau yang sering di sebut sebagai fungsi hash merupakan sebuah algoritma yang mengubah teks atau pesan menjadi sederetan karakter acak yang memiliki jumlah karakter yang sama (Ratno Prasetyo, 2016) yang dipublish oleh National Institute Of Standard and Technology (NIST) pada tahun 2001. SHA sendiri mempunyai beberapa jenis yaitu SHA-0, SHA-1 dan SHA-2. Untuk penelitian ini penulis memilih SHA-2 yang memiliki beberapa fungsi hash dengan *digest* yaitu 224, 256, 384 dan 512 bits atau SHA-224, SHA-256, SHA-384 dan SHA-512.

Algoritma kriptografi modern simetri tersebut terbukti pernah dipakai pada penelitian terdahulu mengenai pengamanan data oleh (Muammar Renaldy, 2015) Penelitian tersebut membahas tentang Implementasi Kriptografi Pada Diary Berbasis Mobile Android Dengan Menggunakan Metode AES dan SHA-1 pada Universitas Budi Luhur. Penelitian tersebut menguji metode AES dan SHA untuk mengkripsi aplikasi S-Diary. Dan algoritma AES ini juga pernah di gunakan oleh (Hadi Fajar, 2019) dalam penelitiannya yaitu Aplikasi Pengamanan File dan Pesan Teks Menggunakan Algoritma AES 256 dan SHA 256 Berbasis Android pada Universitas Pembangunan Nasional "Veteran" Jakarta.

Berdasarkan latar belakang permasalahan diatas maka penelitian yang dilakukan mengambil judul "Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File".

1.2 Identifikasi Masalah

Berdasarkan uraian diatas, maka dapat disimpulkan indentifikasi masalah sebagai berikut.

1. Kebocoran data file yang bersifat sensitif sering terjadi dalam kehidupan sehari hari dan menimbulkan kerugian untuk pihak yang dirugikan serta belum adanya penerapan yang baku untuk pengamanan data file penting pada Universitas Bhayangkara.
2. Di perlukannya sebuah aplikasi baku untuk pengamanan data file untuk menjaga kerahasiaan data tersebut dan belum adanya aplikasi pengamanan file pada Universitas Bhayangkara Jakarta Raya berbasis desktop.

1.3 Rumusan Masalah

Berdasarkan kesimpulan diatas, maka ditetapkan rumusan masalah dalam penelitaan ini sebagai berikut.

1. Bagaimana **Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File?**
2. Bagaimana **Perancangan Aplikasi Untuk Pengamanan Data File Menggunakan AES-256 Dengan Mode CBC dan SHA-256?**

1.4 Tujuan dan Manfaat

Maksud dari penulis dari penelitian pada pengamanan data di Universitas Bhayangkara adalah sebagai berikut.

1. Menerapkan algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) dalam pengamanan data file penting Lembaga kedalam aplikasi yang dibuat oleh penulis yang dinamai *Secret Fichier*. *Secret Fichier* sendiri adalah Bahasa Perancis yang berarti *Secret* yaitu rahasia dan *Fichier* berarti file. Jadi yang dimaksudkan *Secret Fichier* ialah file rahasia.

Sedangkan maksud dan tujuan penulisaan ini adalah untuk memenuhi syarat Skripsi pada Semester Tujuh Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.

1.5 Batasan Masalah

Pembatasan permasalahan diharapkan tidak menyimpang dari pokok permasalahan, sehingga dalam penyeselesaian masalah ini akan dibatasi dimana ruang lingkup penelitian dilakukan untuk divisi administrasi dalam pengamanan data file penting lembaga yang dituangkan kedalam pembuatan aplikasi enkripsi dan deskripsi berbasis desktop. Adapun batasan masalah dalam pengimplementasian algoritma dari AES-256 dengan mode CBC dan SHA-256 ke dalam aplikasi enkripsi dan deskripsi berbasis desktop di sistem operasi Windows. Maka dari itu pembatasan tersebut akan dijelaskan dibawah ini :

1. Proses enkripsi dan deskripsi menggunakan algoritma AES dengan panjang kunci 256 bit dengan mode operasi CBC. Dan untuk Teknik memasukan kunci, dilakukan dengan proses hashing menggunakan SHA agar dapat menghasilkan kunci sebesar 256 bit.
2. Aplikasi enkripsi dan deskripsi Secret Fichier hanya dapat mengenkripsi dan mengdeskripsi file tunggal (bukan folder).
3. Aplikasi enkripsi dan deskripsi Secret Fichier ini mencakup data yang berjenis dokumen, gambar, suara dan video.
4. Untuk mengdeskripsi suatu file digunakan password (kunci) yang sama pada saat si pengguna mengenkripsi file tersebut.
5. Penulis menerapkan algoritma AES-256 mode CBC dan SHA-256 kedalam aplikasi dan menjelaskan tahapan tahapan algoritma tersebut bekerja kedalam penulisan ini.

1.6 Tempat dan Waktu Penelitian

Penelitian dilakukan di Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan, Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia. Selama empat bulan yaitu dari September 2020 sampai Desember 2020.

1.7 Sistematika Penulisan

Penelitian ini akan dibagi menjadi lima bab gambaran masing masing bab akan dijelaskan dibawah ini.

BAB I : PENDAHULUAN

Dalam bab ini berisi penjelasan tentang latar belakang masalah, maksud dan tujuan penelitian, rumusan masalah, pembahasaan masalah, metode pengumpulan data dan sistematika penulisan.

BAB II : LANDASAN TEORI

Dalam bab ini menjelaskan tentang memuat tinjauan dan ulasan singkat mengulas pentinnya penelitian yang dilakukan dan menyampaikan teori yang berhubungan dengan permasalahaan yang dibahas sebagai dasar analisa permasalahaan yang diteliti.

BAB III : METODOLOGI PENELITIAN

Dalam bab ini membahas tentang pendekatan studi dan dapat beruba analisis teori, metode eksperimen, kombinasi, rancangan, spesifikasi sistem baik perangkat keras maupun perangkat lunak.

BAB IV : PERANCANGAN SISTEM DAN IMPLEMENTASI

Dalam bab ini membahas mengenai penerapaan algoritma AES dan SHA serta perancangan aplikasi meliputi perangkat lunak berbasis dekstop, pengujian dan implementasi serta hasil keluaran dari sistem aplikasi yang telah dibuat dan di bahas sesuai penelitian dan hipotesis untuk menjawab permasalahan yang ada.

BAB V : PENUTUP

Dalam bab ini memuat beberapa kesimpulan yang di dapatkan dari penelitian dan menjawab tujuan penelitian atau hipotesis. Serta memuat saran saran yang dapat dikembangkan atau dilakukan sebagai penerapan untuk perusahaan kedepannya.