BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan informasi memberikan perubahan pada masyarakat untuk memperoleh kebutuhan informasi secara cepat dan murah. Informasi yang didapatkan bisa berbentuk data, gambar, maupun suara. Kerahasian dan keamanan data yang berupa informasi ini merupakan bagian terpenting bagi setiap orang. Oleh karenanya penyalahgunaan data atau bocornya informasi merupakan hal yang harus dihindari agar kerahasian dan keamanan data tetap terjaga. Untuk mewujudkan keamanan data dan informasi yang baik dibutuhkan penyandian pada saat proses pengolahan data dimana data yang ada diubah menjadi bentuk data lain yang tidak dapat dimengerti oleh pihak lain. Kriptografi menjadi dasar bagi keamanan komputer dan menjadi salah cara yang paling banyak digunakan untuk mengamankan komputer. Data-data yang diamankan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut. Hal ini dikenal dengan proses enkripsi. Data atau pesan yang asli sering disebut sebagai *plaintext* dan data yang telah di-enkripsi disebut sebagai *chipertext* atau menurut terminoligi yang lebih tepat *enchiper*. Data yang telah dienkripsi disebut *chipertext* karena data asli (*plaintext*) telah mengalami proses di dalam sebuah algoritma kriptografi atau lebih dikenal dengan nama *chiper*.

Kebalikannya, proses merubah pesan yang telah dienkripsi (*chipertext*) menjadi pesan asli (*plaintext*) disebut sebagai proses dekripsi atau *dechiper*. William Stallings mendefinisikan kriptografi sebagai "*the art and science of keeping messages secure*".

Dalam kriptografi terdapat beberapa algoritma yang dapat menyandikan data. Algoritma yang paling dikenal adalah algoritma DES (*Data Encryption Standard*). DES ditetapkan sebagai standard untuk melindungi data dan informasi. Tetapi, DES dianggap sudah tidak aman lagi, karena dengan perangkat keras khususnya kuncinya dapat ditemukan dalam waktu beberapa hari. Kemudian IBM yang membuat algoritma DES dan mengembangkan DES menjadi 3DES (*Triple Data Encryption Standard*). 3DES juga banyak digunakan dan penggunaannya lebih aman dibandingkan DES (Akik Hidayat, 2010).

Banyak para pengguna media sosial sering mempublikasikan foto-foto atau gambar ke internet untuk mengabadikan momen dari suatu kejadian. Momen tersebut di upload ke media publik sehingga orang lain bisa melihatnya. Gambar yang di upload bisa berupa foto pribadi, keluarga, ataupun dokumen penting dalam bentuk *image*. Sebagian dari pengguna yang gemar mengupload gambar meraka ke publik, hanya tahu bahwa gambar mereka sudah di upload yang artinya tersimpan di media tertentu, dimana gambar tersebut bisa dilihat kapan saja dan di download kembali jika dibutuhkan. Namun sebenarnya ada beberapa hal yang sangat beresiko jika mengupload gambar ke media publik misalnya, gambar yang di upload bisa saja di

unduh oleh pihak lain yang dimanfaatkan untuk maksud tertentu. Tentunya suatu keuntungan juga jika kita mempunyai tempat lain untuk menyimpan data kita selain media penyimpanan lokal saja, namun jika konten yang menyimpan data kita rusak tentunya akan menjadi kerugian juga buat kita. Kemudian hal yang yang paling beresiko, biasanya gambar disimpan dalam bentuk album yang menandai letak posisi penyimpan gambar di media publik, letak penyimpanan tersebut bisa saja di akses untuk di unduh semua datanya atau bahkan dihapus oleh pihak tertentu.

Letak penyimpanan data gambar pada media publik berupa link direktori atau sering di sebut *Uniform Resource Locator* (URL). URL berarti suatu "*pathname*" untuk mengidentifikasi sebuah dokumen di web. Didalam URL terdapat informasi nama mesin/*host* (dalam hal ini komputer) yang akan diakses, nama dokumen beserta logical *pathname*-nya serta jenis protokol yang akan digunakan untuk melakukan akses ke web. Pengertian URL adalah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di Internet. URL pertama kali diciptakan oleh Tim Berners-Lee pada tahun 1991 agar penulis-penulis dokumen dokumen dapat mereferensikan pranala ke *World Wide Web*. Sejak 1994, konsep URL telah dikembangkan menjadi istilah *Uniform Resource Identifier* (URI) yang lebih umum sifatnya. Contoh dari URL, misalnya http://mail.google.com/mail/ (Diwarta, 2012).

Fungsi atau kegunaan URL adalah:

1. Sebagai pengidentifikasi sebuah dokumen di web.
2. Untuk memudahkan kita dalam mengakses suatu dokumen melalui *website*.
3. Untuk memberikan penamaan terhadap suatu file / dokumen pada *website*.
4. Memudahkan kita untuk mengingat suatu alamat *website* (Diwarta, 2012).

Jadi dalam penelitian ini, akan dibangun suatu sistem yang bisa menyimpan foto galery, namun diterapkan juga sistem keamanannya dengan menggunakan algortima 3DES yang bisa menyandikan *pathname* dari suatu URL ke bentuk lain yang tidak bisa di lihat dan di akses oleh pihak lain tidak bertanggung jawab. Kemudian, dalam pembahasan penelitian akan dibahas juga tentang analisis sistem yang dibuat, sehingga bisa mengetahui sejauh mana penelitian ini berlangsung.

1.2 Rumusan Masalah

Terdapat rumusan masalah yang akan dilakukan dalam penelitian ini, yaitu sebagai berikut :

1. Bagaimana cara kerja penyimpan foto galery yang tersimpan di media publik bisa terjaga keamananya, namun tetap bisa dilihat dan dipergunakan oleh pengguna, dalam hal ini mengamankan *sourcepath* link url nya.
2. Bagaimana hasilnya setelah diterapkan algortima 3DES pada sistem web foto galery yang dibuat.

1.3 Tujuan Penelitian

Tujuan dari pembahasan penelitian ini adalah sebagai berikut:

1. Memberikan gambaran cara kerja proses enkripsi algoritma 3DES untuk mengamankan *sourcepath* link url.
2. Mengetahui hasil tingkat keamanan pada sistem web foto gallery setelah diterapkan algoritma 3DES.

1.4 Batasan Masalah

Untuk menghindari meluasnya materi pembahasan, maka penulis membatasi permasalahan yang mencakup hal-hal sebagai berikut:

1. Tidak membahas perbandingan antar algoritma.
2. Sistem enkrpisi menggunakan algoritma 3DES.
3. Bentuk yang akan di enkripsi berupa link url *image*.
4. Implementasi dengan menerapakan algoritma 3DES padasistem web foto galery dengan bahasa perograman PHP,*databaseenginee* yang digunakan MySql, dan *webserver* yang digunakan dalam pengembangan program adalah *Apache*.

1.5 Manfaat Penelitian

Dari pembuatan skripsi ini diharapkan adanya manfaat penelitian ini adalah mengetahui proses enkripsi yang berguna untuk keamanan suatu data, dalam hal ini keamanan *sourcepath* dari URL.

1.6 Metodologi Penelitian

Tahapan yang akan dilalui pada skripsi ini adalah sebagai berikut:

1. **Studi Literarur,** dilakukan pengkajian mengenai cara pembuatan sistem untuk sistem web foto galery dengan menerapkan algoritma 3DES sebagai keamanan data dari berbagai sumber.
2. **Analisa dan Perancangan Sistem**, dilakukan analisa dan perancangan sistem untuk sistem web foto galery dengan menerapkan algoritma 3DES.
3. **Implementasi Sistem,** dilakukan implementasi berdasarkan hasil analisa dan perancangan sistem web foto galery dengan menerapkan algoritma 3DES.
4. **Pengujian dan Evaluasi**, dilakukan pengujian pada sistem web foto galery yang telah dibuat kemudian hasilnya dievaluasi.

1.7 Sistematika Penulisan

Laporan disusun secara sistematis sehingga mudah dibaca, ditelusuri, dan di evaluasi. Sistematika penulisan laporan skripsi ini terbagi menjadi lima bab sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini menguraikan tentang latar belakang masalah, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Bab ini membahas teori-teori yang mendukung dalam penyusunan skripsi seperti proses enkripsi, penerapan algoritma dan beberapa contoh penelitian yang ada.

BAB III METODE PENELITIAN

Bab ini menguraikan beberapa tahapan penelitian yang dilakukan secara rinci.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menguraikan tahapan yang harus dilalui pada proses mengamankan data, dan mengetahui data-data yang digunakan pada proses tersebut, sampai menghasilkan data yang lebih aman.

BAB V KESIMPULAN DAN SARAN

Bab ini menguraikan beberapa kesimpulan dari hasil penelitian untuk menjawab rumusan masalah. Pada bagian saran, diisi rekomendasi dari penulisan untuk penelitian selanjutnya.