BAB I

PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Di mana kebenaran dan keaslian suatu informasi sangat penting baik pada saat pengiriman ataupun pada saat informasi tersebut diterima. Pesan, data, atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem lain yang setingkatnya, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini disebabkan oleh adanya kemajuan bidang jaringan komputer dengan konsep *open system*-nya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat pesan, data, atau informasi tersebut tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak.

Dengan adanya sebuah kriptografi yang meliputi proses enkripsi maka pesan, data, maupun informasi dapat dikodekan sehingga orang yang tidak berkepentingan tidak dapat membaca informasi tersebut, selain orang yang mengetahui kunci *(Key)* untuk mendeskripsikannya.

Dengan adanya algoritma-algoritma kriptografi yang berkembang pada saat ini. Di mana masing-masing algoritma tersebut mempunyai kekurangan dan kelebihan. Dengan bertitik tolak pada masalah diatas maka penulis mencoba untuk menggunakan algoritma kriptografi yaitu algoritma GOST . Dari sekian banyak algoritma kriptografi tersebut, di mana masing-masing algoritma mempunyai kelebihan dan kekurangan dalam melakukan proses enkripsi data dan waktu prosesnya.

1.2 Rumusan Masalah

Keamanan dan kerahasian data pada jaringan komputer sangat penting artinya, baik pada saat pengiriman ataupun pada saat data atau informasi tersebut diterima, karena data atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan, dari uraian di atas, maka dapat didefinisikan masalahnya sebagai berikut:

1. Perangkat lunak akan menampilkan tahap – tahap penghitungan dalam bilangan biner.
2. Perangkat lunak memiliki fasilitas untuk menampilkan nilai dari *S-Box* yang digunakan dan teori – teori dasar dari metoda GOST.

3. Perangkat lunak akan menampilkan tahap – tahap enkripsi dan dekripsi.

1.3 Batasan Masalah

Di dalam penyusunan tugas akhir ini, batasan masalah bertujuan untuk memudahkan perancangan dan menghindari adanya kegiatan di luar sasaran yang diinginkan, sehingga diperlukan batasan masalah. Adapun batasan dari penulisan tugas akhir ini adalah sebagai berikut:

1. Pembahasan hanya mengenai algoritma GOST pada proses pengamanan data.
2. Pengujian hanya dilakukan dalam hal kecepatan proses enkripsi dan pengiriman file
3. Hanya mengenkripsi dan dekripsi sebuah file.
4. File data terenkripsi (*ciphertext*) tidak dapat dienkripsi lagi.

1.4 Tujuan Penelitian

1. Sebagai salah satu syarat menyelesaikan pendidikan S1 pada program studi teknik informatika.
2. Untuk menerapkan dan mengembangkan teori yang didapat di bangku perkuliahan.
3. Mengurangi orang yang tidak berkepentingan

1.5 Manfaat Penelitian

1. Memperoleh gelar sarjana komputer pada STMIK AMIKOM YOGYAKARTA.
2. Melakukan keamanan dalam mengirim informasi.

1.6 Metodologi Penelitian

Kegiatan pembandingan dua algoritma pengamanan data yaitu algoritma GOST untuk pemecahan masalah yang ada, yaitu mengetahui kekurangan dan kelebihan dari masing-masing algoritma, maka dilakukan analisis terhadap algoritma tersebut.

Tahapan yang dilaksanakan pada saat penelitian adalah sebagai berikut:

1. Mempelajari algoritma kunci simetris dengan menggunakan mode operasi CFB (Cipher Feedback), dalam hal ini yang dibahas adalah algoritma Gost.
2. Merancang suatu sistem pengamanan data dengan menggunakan algoritma Gost yang dapat mengenkripsi dan mendekripsi data yang diimplementasikan dalam bahasa pemrograman Visual Basic
3. Melakukan uji program.
4. Membuat kesimpulan dan saran dari penelitian yang dilakukan.
5. Menyelesaikan penyandian pesan dengan menggunakan *algoritma Gost* pada *mode cipher feedback* (*CFB*).
6. Melakukan perancangan dan menerapkan *algoritma Gost* pada *Mode Cipher Feedback* (*CBF*) dengan menggunakan bahasa pemrograman Visual Basic.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir yang' disusun adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini terdiri atas latar belakang, maksud dan tujuan dari penulisan tugas akhir, metodologi penelitian yang diterapkan, batasan masalah, serta sistematika penulisan tugas akhir ini

BAB II LANDASAN TEORI

Bab ini membahas mengenai kriptografi secara umum, enkripsi dan deskripsi, jaringan dengan algoritma GOST.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan membahas mengenai permasalahan keamanan data pada komputer dan pemecahan masalahnya dengan menggunakan algoritma Gost, serta menganalisa pemrosesan kunci, proses enkripsi dan dekripsi serta kekurangan dan kelebihan dari masing-masing algoritma di dalam melakukan penyandian data. serta bagaimana proses enkripsi dan dekripsi yang akan dilakukan oleh program.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Menjelaskan implementasi perancangan algoritma GOST dan membahas serta menganalisa hasil penelitian tersebut.

BAB V PENUTUP

Bab ini berisi kesimpulan serta saran-saran untuk pengembangan dan perbaikan.