IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DOKUMEN MENGGUNAKAN ALGORITMA GOST

Heni Pratiwi
035314012

ABSTRAKSI

Jika ada data penting yang harus dilindungi kerahasiaannya, maka diperlukan suatu teknik untuk mengamankan data tersebut. Salah satu teknik yang digunakan yaitu dengan melakukan enkripsi. Enkripsi adalah teknik pengkodean data oleh algoritma tertentu yang membuat data tidak bisa dibaca oleh program apa saja tanpa kunci *decryption*. Enkripsi juga dapat digunakan untuk melakukan proteksi pada saat data ditransmisikan melalui jalur komunikasi. Salah satu teknik enkripsi yang digunakan adalah *symmetric encryption*, yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Kunci simetris *(symmetric encryption)* yang digunakan merupakan kesepakatan antara pengirim dan penerima pesan.

Dalam tugas akhir ini akan menggunakan Algoritma *Gost*. Algoritma ini termasuk dalam *symmetric encryption*. Algoritma ini dapat mengkodekan isi berkas dokumen asli dalam kode-kode tertentu agar tidak bisa dibaca orang lain yang tidak berhak. Algoritma ini merupakan blok cipher 64 bit dengan panjang kunci 256 bit. Pada tugas akhir ini akan menggunakan bahasa pemrograman Delphi. Dalam tugas akhir ini akan mencari kecepatan proses dan rerata rasio ketiga tipe berkas (.txt,.doc,.rtf). Berkas dokumen yang digunakan untuk uji coba berjumlah enam buah dengan berbagai ukuran.

Percobaan dilakukan sebanyak tiga kali untuk masing-masing berkas, lalu diambil rata-rata waktunya. Kemudian dari rata-rata waktu tersebut dapat dihitung rerata waktu dan rerata rasio untuk ketiga tipe berkas. Hasil percobaan menunjukkan bahwa semakin besar ukuran berkas maka semakin lama pula waktu prosesnya.

IMPLEMENTATION OF DOCUMENTS ENCRYPTION AND DECRYPTION USING GOST ALGORITHM

Heni Pratiwi
035314012

ABSTRACT

If any important data that must be protect, then it will be need some technique to save the data. One of technique is encryption. Encryption is data coding of some algorithm which can make the data unreadable without decryption key. Encryption also can protect the data when its transferred in communication network. One of techniques of encryption is symmetric encryption, which using the same key for encryption and decryption processing. But first, sender and receiver have a deal for the key that used for this encryption.

On this final project will use Gost Algorithm. This algorithm include in *symmetric encryption.* This algorithm can make some code in original documents which can not read for someone else who don't have right. This algorithm have 64 cipher block with key length 256 bit. This final project will use Delphi programming language. On this final project will looking for the speed of time and rasio average between three type of documents (.txt,.doc,.rtf). There are six documents that used on this project with various size.

There are three times for testing for each documents, then get the time average. After that, it can use to calculate the time average and ratio average for the three type of documents. The result of testing show that the bigger the size of documents the longer the time.