ABSTRAK

Pada proses pengiriman data terdapat beberapa aspek keamanan yang perlu diperhatikan yaitu : *Confidentiality*, *Authentication*, *Integrity*, *Nonrepudiation*, *Access Control*, dan *Availability*. Untuk menjaga kerahasiaan isi data dan integritas suatu data dibutuhkan proses penyandian atau pengkodean data sebelum dilakukan proses pengiriman data. Salah satu hal yang dapat dilakukan untuk meningkatkan keamanan data yaitu dengan menggunakan metode yang dikenal dengan istilah Kriptografi. Dalam kriptografi sendiri terdapat berbagai algoritma antara lain algoritma IDEA, DES, AES, Blowfish, 3DES, RSA, dan lain-lain.

Banyak algoritma kriptografi yang telah ada. Tetapi kebanyakan jika algoritmanya sangat kompleks, pasti membutuhkan waktu dan penggunaan memori yang besar untuk melakukan proses enkripsi – dekripsi. Ini yang menjadi kendala jika ingin aman tapi tidak efisien. Tetapi jika efisien belum tentu aman. Semakin aman suatu algoritma, semakin lama waktu yang dibutuhkan untuk proses enkripsi – dekripsinya. Begitu juga sebaliknya.

Dalam tugas akhir ini akan menggabungkan algoritma IDEA dan algoritma Blowfish sebagai algoritma hibrid dimana pemilihan algoritma dipilih berdasarkan kemudahan penerapan algoritma, kecepatan eksekusi serta penggunaan memori. Dengan penggabungan algoritma ini diharapkan nantinya tercipta algoritma yang mudah dipahami dan efektif untuk diterapkan di berbagai aplikasi enkripsi-dekripsi khususnya untuk dokumen yang tidak membutuhkan level enkripsi yang terlalu tinggi. Selain itu diharapkan algoritma yang dihasilkan memiliki tingkat keamanan yang baik namun tetap memiliki waktu eksekusi yang singkat dan penggunaan memori yang sedikit.

ABSTRACT

In the data transmission process, there are several security aspects to note are: Confidentiality, Authentication, Integrity, nonrepudiation, Access Control, and Availability. To maintain the confidentiality and integrity of the data content of a data encryption or encoding process takes the data prior to the data transmission process. One of the things that can be done to improve the security of data is by using a method known as cryptography. In itself there are various cryptographic algorithms include the IDEA algorithm, DES, AES, Blowfish, 3DES, RSA, and others.

Many existing cryptographic algorithms. But most if the algorithm is very complex, certainly takes time and large memory usage to make the process of encryption - decryption. It is a constraint if you want a safe but inefficient. But if efficient is not necessarily safe. The more secure the algorithm, the longer it takes for the process of encryption - decryption. Vice versa, the less time is needed, not necessarily secure an algorithm.

In this final project will combine the IDEA algorithm and the Blowfish algorithm as a hybrid algorithm where choice of algorithm selected based on ease of implementation of the algorithm, the execution speed and memory usage. With the incorporation of this algorithm is expected to eventually create an algorithm that is easy to understand and effective to be applied in a variety of encryption and decryption applications, especially for documents that do not require encryption level is too high. Also expected resulting algorithm has a good level of security but still have a short execution time and memory usage slightly.