

ABSTRAKSI

Seiring dengan perkembangan informasi, maka keamanan data menjadi masalah yang penting, terutama pada jaringan komputer. Pengamanan data dapat membantu dalam menjaga kerahasiaan data agar tidak dapat dibaca oleh orang yang bukan merupakan penerima yang diharapkan. Untuk mengatasi hal tersebut banyak usaha yang dilakukan untuk melindungi keaslian dan kerahasiaan data, terlebih lagi untuk data yang sangat penting. Salah satu sarana pengamanan data adalah dengan teknik kriptografi dengan metode enkripsi.

Dengan metode enkripsi data maka si penerima data bisa yakin bahwa data yang diterimanya benar berasal dari pengirim yang sesungguhnya. Metode yang digunakan adalah dengan merubah teks menjadi suatu teks acak yang tidak dapat dibaca oleh siapapun, kecuali dengan mendekripsinya terlebih dahulu. Oleh karena itu diperlukan suatu algoritma untuk menghasilkan kunci yang sangat rahasia yang akan digunakan dalam proses enkripsi dan dekripsi.

Pembuatan aplikasi enkripsi-dekripsi data ini akan menyulitkan dan merepotkan programmer dalam mengembangkan aplikasi, hal ini disebabkan programmer harus mengetikkan kode program yang cukup panjang pada saat pembuatan software. Dari keadaan tersebut maka dapat ditarik kesimpulan bahwa programmer akan mengalami kesulitan menyertakan proses enkripsi-dekripsi pada aplikasi yang dibuat. Oleh karena itu penulis ingin mengimplementasikan suatu komponen tambahan untuk mempermudah dalam pembuatan aplikasi.

Banyak algoritma enkripsi-dekripsi yang dapat digunakan untuk mengamankan / menjaga kerahasiaan data. Algoritma yang akan digunakan dalam pembuatan komponen ini adalah algoritma Blowfish. Alasan memilih algoritma ini karena algoritma ini memiliki kecepatan yang baik dalam menghasilkan panjang kunci yang besar dalam waktu yang lebih cepat daripada algoritma enkripsi-dekripsi yang lain. Secara garis besar algoritma Blowfish terdiri dari 2 bagian, yaitu Key expansion dan Enkripsi data. Key expansion berfungsi untuk merubah kunci yang akan digunakan dalam proses enkripsi. Sedangkan enkripsi data adalah proses untuk merubah teks asli menjadi suatu teks acak. Untuk menghasilkan kembali plaintext asli, akan digunakan algoritma dekripsi dengan kunci yang sama dengan enkripsi.