INTISARI

Topik penulisan ini adalah tentang program enkripsi dan dekripsi suatu berkas. Enkripsi terhadap suatu berkas dilakukan untuk mengubah nilai tiap *byte*-nya sehingga isi pokok dari berkas tersebut dapat disamarkan. Sedangkan proses dekripsi dilakukan untuk mengembalikan isi pokok dari berkas sesuai dengan aslinya. Metode enkripsi yang digunakan adalah metode enkripsi dengan kunci tunggal menggunakan algoritma blok, IDEA (*International Data Encryption Algorithm*). IDEA dikembangkan pada tahun 1990 di Swiss oleh kriptografer ternama, James Massey dan Xuejia Lai. Algoritma ini bekerja pada blok-blok *plaintext* 64 bit. Panjang kunci yang digunakan adalah 128 bit.

Pada waktu pengguna akan melakukan enkripsi ataupun dekripsi, pengguna harus terlebih dahulu memilih berkas yang akan diproses. Berkas yang dipilih merupakan berkas dokumen dan grafis dengan tipe apapun. Hal ini disesuaikan dengan batasan uji coba yang telah ditetapkan, meskipun tidak menutup kemungkinan pengguna dapat mengenkripsi maupun mendekripsi berkas lain. Setelah pengguna telah memilih berkas yang akan diproses, maka selanjutnya pengguna menetapkan kunci yang akan dipakai dan mengkonfirmasikannya kembali. Kemudian pengguna dapat menentukan apakah berkas sumber akan dihapus atau tidak, serta menentukan apakah berkas hasil enkripsi atau dekripsi akan disimpan dalam direktori yang sama dengan berkas sumber atau tidak. Setelah itu proses enkripsi atau dekripsi dapat mulai dilakukan. Fasilitas yang ditambahkan dalam program ini adalah penambahan menu dalam *context menu Windows*. Fasilitas ini ditambahkan supaya pengguna dapat melakukan enkripsi dan dekripsi berkas secara langsung dengan me-*click* kanan berkas tersebut kemudian memilih proses yang akan dilakukan. Program ini dikembangkan dengan menggunakan *Microsoft Visual Basic* 6.0 dan *Windows* API (*Application Programming Interface*).

Dari hasil uji coba tampak bahwa program ini ternyata terbukti bekerja sesuai dengan algoritma IDEA 64-bit, proses enkripsi dan dekripsi terhadap semua jenis berkas dokumen dan grafis juga dapat berjalan dengan baik, dan waktu yang diperlukan untuk melakukan enkripsi dan dekripsi akan linier dengan ukuran berkas yang dipilih.

ABSTRACT

This project was about making a file encryption programming. Encryption for any files is done by changing every single byte of this value, so that substance of that file can be hided. Decryption is the reversed process of encryption. It changes the substance back into the original one. This program is using one of the symmetric algorithm that operates on the plaintext in group of bits, IDEA (*International Data Encryption Algorithm*). IDEA is developed by James Massey and Xuejia Lai in 1990, Swiss. This algorithm operates on 64-bit plaintext blocks. The key is 128 bits long.

When user wants to encrypt or decrypt, user must first choose the file which will be processed. It is made according to the border of the testing that have been decided, although it is not possible that user can encrypt and decrypt the other one. After user have choosed the file that will be processed, user can define the key that will be used and confirm it again. Then user can decide whether erase the source file or not, and decide whether the encrypted or decrypted file will be saved in the same directory with the source file or not. After that, encryption and decryption can be executed. There is a facility that was added on context menu *Windows*, so that the user can do encryption and decryption file just by right-click the file and then choose the process that he/she wants to do. This program is developed using *Microsoft Visual Basic* 6.0 and *Windows* API (*Application Programming Interface*).

From the test result, it seems that this program has been approved working like IDEA 64-bit algorithm, encryption and decryption can be ran so well to any type of files, and the time is needed to encrypt and decrypt will be linear with the size of the chosen file.