

## ABSTRAK

Tidak ada data yang aman dalam jaringan komputer global, usaha *pengamanan data digital* dimaksudkan untuk mengurangi tingkat kebocoran terhadap pihak pengganggu. Oleh karena itu diperlukan metode pengamanan data, salah satunya dengan metode enkripsi. Tugas akhir ini membahas pengamanan data digital berupa file text yaitu dengan menggunakan *metode enkripsi* IDEA. Proses enkripsinya menggunakan XOR, penjumlahan dengan modulo  $2^{16}$ , dan perkalian dengan modulo  $2^{16} + 1$  menurut fungsi  $C = E_k(M)$ . Sandi diperoleh dari pesan plaintext yang berupa 64 bit blok data dan terbagi dalam empat sub blok 16 bit :  $X_1$ ,  $X_2$ ,  $X_3$ , dan  $X_4$ . Selanjutnya diproses sesuai algoritma enkripsi IDEA dengan penjadwalan kunci sepanjang 128 bit yang terbagi menjadi 8 sub kunci 16 bit sebanyak 9 putaran. Proses enkripsi ini menghasilkan *data yang terenkripsi* yang diharapkan aman dari pengganggu. Program enkripsi ini disajikan dalam bentuk Single Data Interface (SDI) yaitu hanya menampilkan satu jendela program untuk mengeksekusi perintah enkripsi atau dekripsi.

## ABSTRACT

There is no secure data on global computer network, the way to protect digital data is purposed to reduce the leaking from adversary. We need some methods to protect the data. One of them is the encryption's method. The final projects discuss about protecting digital data from text file by using IDEA's method in the storage level. The encryption's process is using logical XOR operation, addition with modulo  $2^{16}$  and multiplication modulo  $2^{16} + 1$  agree with function  $C = E_k(M)$ . The ciphertext is result from plaintext that 64 bit data blocks and divided in to four 16 bit sub blocks :  $X_1$ ,  $X_2$ ,  $X_3$ , and  $X_4$ , then process agree with IDEA encryption algorithm by key scheduled 128 bit key divided by eight sub keys 16 bit and using 9 rounds. This encryption process result the encrypted data that is hoped secure from adversary. This encryption program is presented in a Single Data Interface (SDI) which only show one program window to execute either encrypt or decrypt order.