ABSTRAK

Tidak ada data yang aman dalam jaringan komputer global, usaha *pengamanan data digital* dimaksudkan untuk mengurangi tingkat kebocoran terhadap pihak pengganggu. Oleh sebab itu diperlukan metode pengamanan data, salah satunya dengan metode enkripsi. Tugas akhir ini membahas pengamanan data digital berupa file teks yaitu dengan menggunakan *metode enkripsi DES*. Proses enkripsinya menggunakan operasi logika XOR, yang dikombinasikan dengan proses permutasi, substitusi, dan ekspansi menurut fungsi $L_{i-1} \oplus f(R_{i-1},K_i)$ dimana $f(R_{i-1},K_i) = (P(S(E(R_{i-1})\oplus K_i)))$. Sandi diperoleh dari pesan plaintext yang dipermutasikan kemudian dibagi dua L_0 *dan* R_0 selanjutnya diproses sesuai algoritma enkripsi DES dengan kontrol pemasukan kunci. Dan sebaliknya pesan plaintext diperoleh dengan mendekripsi sandi menggunakan algoritma dan kunci yang sama. Proses enkripsi ini menghasilkan *data yang terenkripsi* yang diharapkan aman dari pengganggu.

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 project discuss about protecting digital data from text file by using DES's method in the storage level. The encryption's process is using logical XOR operation, combinated with permutation, substitution, and expantion process agree with function $L_{i-1} \oplus f(R_{i-1},R_i)$ that $f(R_{i-1},R_i) = P(S(E(R_{i-1}) \oplus K_i))$. The ciphertext is result from plantext order permuted then divided by two L_0 and R_0 then process agree with DES encryption algorithm by control the entering key. And the otherwise, plantext message is resulted by decrypte ciphertext using the same algorithm and key. This encryption process result the encrypted data that is hoped secure from adversary.