# ABSTRAK

Untuk mengamankan data/informasi dari pihak pengganggu diperlukan metode pengamanan data dan salah satunya dengan metode enkripsi. Tugas akhir ini membahas pengamanan data digital berupa file teks yaitu dengan menggunakan metode enkripsi GOST (*Gosudarstvennyi Standard*). Proses enkripsinya menggunakan operasi logika xor, yang dikombinasikan dengan proses substitusi, dan transposisi menurut fungsi $L_{r-1}$ *xor* $f(R_{r-1},K_r)$ dimana $f(R_{r-1},K_r) = (T(S(R_{r-1}$ *xor* $K_r)))$. Sandi diperoleh dari pesan plainteks yang dibagi dua menjadi $L_0$ dan $R_0$ selanjutnya diproses sesuai algoritma enkripsi GOST dengan kontrol pemasukan kunci. Proses enkripsi ini menghasilkan data yang terenkripsi yang diharapkan aman dari pengganggu. Dan sebaliknya pesan plainteks diperoleh dengan mendekripsi sandi menggunakan algoritma dan kunci yang sama.

## ABSTRACT

The efforts to keep the data being leaked to the adversary, it is need such methods that can keep it secure, and one of them is the encryption's method. This final project explain about digital data security precisely on the text file with GOST (*Gosudarstvennyi Standard*) method. The encryption's process is using logical operation xor, combinated with substitution, and transposition process agree with function $L_{r-1}$ *xor* $f(R_{r-1},K_r)$ that $f(R_{r-1},K_r) = (T(S(R_{r-1}$ *xor* $K_r)))$. The ciphertext is result from plantext divided by two $L_0$ and $R_0$ then process agree with GOST encryption algorithm by control the entering key. This encryption process result the encrypted data that is hoped secure from adversary.And the otherwise, plantext order is resulted by decrypte ciphertext using the same algorithm and key.