# ABSTRAK

Pemanfaatan internet untuk bertukar informasi atau dalam mengirim pesan, telah memberi banyak perubahan dalam kehidupan manusia. Pertukaran informasi dapat dilakukan dengan cepat walaupun dari jarak yang jauh. Dalam hal ini, masalah keamanan data sangat diperlukan untuk menjamin kerahasiaan informasi atau data yang dikirim.

Salah satu cara untuk menjamin kerahasiaan data adalah dengan melakukan teknik kriptografi. Kriptografi adalah ilmu untuk menjaga keamanan data sehingga hanya user yang berhak saja yang dapat melihat isi dari data yang dikirim. Dalam algoritma kriptografi terdapat beberapa metode utama, salah satunya adalah algoritma simetrik. Standar yang biasa dipakai dalam algoritma simetrik adalah DES, CAST, Blowfish, RC dan AES.

Dalam tugas akhir ini dibuat komponen pengaman data dengan algoritma RC6. Input dan output dari algoritma RC6 terdiri dari urutan data sebesar 128 bit.Proses enkripsi algoritma RC6 dimulai dengan mencari ekspansi kunci (*key expansion)*. Komponen yang dibangun ini dapat menerima inputan (*plaintext*) berupa string, bilangan heksadesimal, ASCII atau pun biner dan menghasilkan *chipertext* berupa bilangan heksadesimal.

Uji coba dilakukan melalui tahap verifikasi yang bertujuan untuk mengetahui apakah komponen ini dapat menghasilkan *plaintext* yang sama sebelum proses enkripsi dengan *plaintext* yang dihasilkan dari proses dekripsi, dan validasi dilakukan oleh beberapa programmer untuk memastikan komponen yang dibuat sesuai dengan sistem yang berjalan/diinginkan. Dari uji coba ini dapat diambil kesimpulan bahwa komponen ini telah berjalan dengan benar.