# ABSTRAK

Komunikasi data antar sistem komputer memerlukan adanya usaha menjaga kerahasiaan dan keamanan data. Salah satu cara menjaga kerahasiaan data adalah dengan menggunakan kriptografi yaitu ilmu yang mempelajari penulisan secara rahasia. Dengan kriptografi, data sederhana (*Plaintext*) diubah menjadi bentuk yang tidak dapat dipahami (*Ciphertext*) sehingga tidak dapat dibaca oleh orang yang tidak sah atau dengan kata lain kerahasiaan data terjaga. Proses ini dikenal dengan enkripsi (Encryption). Data yang telah berubah bentuk (*Ciphertext*) tersebut hanya dapat dibaca oleh orang yang memiliki kunci (*key*). Kunci diperlukan untuk merubah kembali ciphertext ke bentuk data yang sebenarnya. Proses ini disebut dengan dekripsi (*Decryption*)

Tugas Akhir ini mempelajari dan mengimplementasikan suatu algoritma kriptografi dalam penyandian data dengan menggunakan algoritma block cipher SAFER+. Algoritma SAFER+ merupakan salah satu kandidat kuat *Advanced Encryption Standard (AES)* yang dipersiapkan untuk menggantikan *Data Encryption Standard (DES)*

Pada tugas akhir ini juga dianalisa kekuatan dan kelemahan dari algoritma kriptografi SAFER+ yang dibandingkan dengan algoritma lain (CAST-256 dan LOKI97), sehingga dapat dipertimbangkan kemungkinan penggunaannya sesuai kebutuhan atau sebagai alternatif pengganti dari algoritma yang sudah ada. Parameter analisis yang dilakukan mencakup waktu dan avalanche effect.. Berdasarkan penelitian yang telah dilakukan, pada akhirnya didapat bahwa CAST-256 secara umum menunjukkan hasil yang lebih baik.

**Keyword :**

- Block Cipher
- SAFER+
- Kriptografi