# ABSTRAK

Melindungi data dari suatu serangan merupakan hal yang penting dalam proses pertukaran informasi. Oleh karena itu diperlukan suatu metode untuk menjaga keamanan dan kerahasiaan data, agar data tersebut hanya dapat diakses oleh orang-orang tertentu. Kriptografi merupakan sebuah metode dengan cara menyembunyikan informasi dari pihak ketiga.

Untuk mengamankan sebuah data yang *real-time* diperlukan suatu algoritma yang memiliki tingkat kualitas dan keamanan yang optimal. Algoritma yang digunakan adalah AES (*Advanced Encryption Standard)*. AES adalah algoritma kriptografi berbasis *chipertext* simetrik yang dapat mengenkripsi dan dekripsi *video surveillance*. AES memiliki sifat cipher yang diharapkan yaitu: tahan menghadapi analisis sandi yang diketahui serta fleksibel digunakan dalam berbagai perangkat keras dan perangkat lunak. Algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi.

Pada penelitian Tugas Akhir ini dirancang suatu program aplikasi berbasis Java Dekstop.Terdapat dua program aplikasi yaitu, aplikasi Server dan aplikasi Client. Program aplikasi ini digunakan untuk mengirimkan video yang direkam dengan menggunakan *webcam* laptop secara *real-time.* Pengujian dilakukan dengan dua cara melalui *live streaming* dari webcam dan mengirmkan file standar Movie.Mjpeg

Hasil dari penelitian diperoleh hasil delay paling bagus untuk live streaming 0,08 sekon , untuk mengirimkan file Movie.Mjpeg .0,04 sekon. Pengujian untuk Avalanche Effect memperoleh hasil yang baik yaitu 59,375%. Hasil dari Normalized Correlation untuk live streaming adalah 0,119 dan mengirimkan file Movie.Mjpeg adalah 0.

**Kata kunci: Kriptografi, AES, *video surveillance, live streaming***