

ABSTRAK

Instant messaging (IM) saat ini sangat diminati oleh seluruh kalangan penduduk dunia, termasuk di Indonesia. Sebagian besar masyarakat yang menggunakan *smartphone* menggunakan aplikasi ini sebagai sarana untuk mempermudah komunikasi. Dengan maraknya penggunaan IM, maka aspek keamanan data atau informasi pada IM juga perlu dipertimbangkan. Oleh sebab itu, penggunaan sistem enkripsi pada IM sangat dibutuhkan untuk menjaga keamanan data atau informasi saat berkomunikasi.

Algoritma enkripsi dan dekripsi yang akan digunakan adalah Algoritma AES-128. Algoritma ini merupakan algoritma *stream cipher* dan menggunakan kunci simetris 128-bit. Dengan menggunakan algoritma ini, data atau informasi yang akan dikirim ke penerima akan lebih aman.

Sistem enkripsi dan dekripsi menggunakan algoritma AES-128 ini akan diimplementasikan pada aplikasi *Prototype Community Messenger* berbasis sistem operasi *Android* yang memiliki performansi baik, terlihat dari nilai *Avalanche Effect* dengan rata-rata bernilai 0,539069. Perbandingan waktu enkripsi dan dekripsi pesan, dimana semakin banyak masukkan pesan oleh pengguna maka waktu enkripsi dan dekripsi semakin lama.

Kata kunci : *instant messaging* (IM), enkripsi, algoritma AES-128, android