

## ABSTRAK

Saat ini, perkembangan teknologi komunikasi semakin lama semakin maju dan kebutuhan akan keamanan dalam komunikasi semakin tinggi, sehingga dibutuhkan suatu aplikasi yang dapat memenuhi kebutuhan tersebut. Aplikasi *chatting* merupakan salah satu media komunikasi yang cepat, *simple* dan hemat biaya yang diharapkan dapat memenuhi kebutuhan tersebut.

Pada tugas akhir ini dilakukan perancangan dan implementasi aplikasi *chatting* dengan menggunakan algoritma *enkripsi*. Algoritma *enkripsi* yang digunakan pada perangkat lunak adalah algoritma *blowfish*, karena algoritma *blowfish* cepat, sederhana, berlisensi bebas sehingga *open source* serta tidak banyak memakan *resources* dalam *enkripsi* data. Perangkat lunak menggunakan bahasa pemrograman Java, hal ini ditujukan agar perangkat lunak bersifat *platform independent*. Pengujian perangkat lunak dilakukan terhadap pengujian performa algoritma *blowfish*, pengujian *alpha* dan *beta*.

Hasil dari pengujian *alpha* menunjukkan, bahwa perangkat lunak berfungsi dengan baik secara fungsional (program bebas dari kesalahan). Hasil dari pengujian *beta* menunjukkan bahwa perancangan sistem aplikasi menghasilkan aplikasi yang sesuai dengan spesifikasi perancangan yang telah dirancang. Dari segi keamanan, terbukti data yang dikirim melalui jaringan yaitu *ciphertext* (*plaintext* yang telah di-*enkripsi*), rata-rata waktu proses *enkripsi* 0.111 milidetik dan rata-rata waktu proses *dekripsi* 0.251 milidetik, serta *avalanche affect* membuktikan bahwa algoritma *blowfish* memenuhi syarat sebagai algoritma kriptografi yang baik. Jadi, aplikasi *chatting* “VicChat” aman dari *cryptoanalyst* atau *sniffer*.

**Kata Kunci :** *Chatting, Enkripsi-Dekripsi, Algoritma Blowfish, J2SE.*