ABSTRAK

Algoritma *twofish* menggunakan struktur yang kompleks dan acak, sehingga sangat sulit untuk dipecahkan & cocok dimanfaatkan untuk enkripsi dan dekripsi pesan teks dan *file* gambar. Metode penelitian meliputi studi literature, perancangan *software,* pengujian system, pengambilan data, analisis data, kesimpulan dan saran. Percobaan dilakukan dengan berbagai panjang karakter dimulai dari 20 hingga 200 karakter dan ukuran *file* gambar dimulai dari 8811 *byte* hingga 6.268.405 *byte* untuk mengamati waktu yang dibutuhkan, ukuran *chipertext*, dan kecepatan proses enkripsi dan dekripsi. Beberapa contoh algoritma kriptografi dengan kunci simetris yaitu *twofish, blowfish,* dan *serpent*, dari ketiga algoritma tersebut, *twofish* terbukti lebih cepat dalam melakukan enkripsi sebesar 35% dan dekripsi sebesar 43%, namun memiliki kekurangan dalam manajemen kunci yang sulit, seperti kunci *twofish* yang panjang antara 128, 192, atau 256 bit & kompleksitas algoritma *twofish* yang membutuhkan pemahaman yang mendalam tentang algoritma ini. Pada *twofish* juga terdapat beberapa blok pembangun yang akan dibahas pada penelitian ini, yaitu *S-Boxes, MDS Matrices*, Transformasi Pseudo-Hadamard (PHT), *whitening* dan penjadwalan kunci. Hasil dari penelitian ini menunjukan bahwa proses enkripsi dan dekripsi memerlukan waktu sekitar 2 hingga 13 detik untuk teks dan sekitar 0,06 hingga 630 detik untuk *file* gambar. Didapatkan juga hasil yang lebih cepat enkripsi-dekripsi gambar dibanding teks untuk ukuran yang sama, sebagai contoh enkripsi-dekripsi gambar dengan ukuran 2230 *byte* dan teks dengan ukuran 2230 *byte*, untuk gambar memerlukan waktu 0,038 detik, sedangkan untuk teks memerlukan waktu 141 detik, yang berarti enkrpisi dekripsi gambar lebih cepat disbanding teks.

Kata Kunci: dekripsi, enkripsi, kriptografi *Twofish.*