ABSTRAKSI

Perkembangan teknologi informasi yang sangat pesat dewasa ini menyebabkan informasi menjadi barang yang berharga, oleh karena itu perlu dilakukan perlindungan terhadap informasi dengan pelbagai cara. Salah satu cara lazim untuk melindungi data adalah kriptografi. Kriptografi sendiri merupakan cabang dalam ilmu matematika yang memanfaatkan proses komputasi untuk mengacak data, yang bertujuan untuk mencegah pihak-pihak yang tidak diizinkan untuk mengetahui atau memodifikasi data tersebut.

Dalam algoritma kriptografi, secara umum dapat dibedakan berdasarkan pertukaran kuncinya, yaitu algoritma kunci simetrik dan algoritma kunci asimetrik. Dalam kedua algoritma tersebut ditemukan beberapa kelemahan, salah satu kelemahan pada algoritma kriptografi simetrik adalah pertukaran kunci yang relatif sulit, sedangkan pada algoritma kriptografi asimetrik waktu enkripsi memakan waktu yang cukup lama. Salah satu solusinya adalah dengan cara pengiriman data menggunakan kunci simetrik dan pengiriman kunci menggunakan kunci asimetrik, hal tersebut dinamakan *hybrid cryptosystem*. Disamping kerahasiaan suatu data diperlukan juga integritas pengirim suatu data dan validitas. Oleh sebab itu, salah satu solusinya adalah *digital signature.*

Algoritma simetrik yang diteliti adalah DES, TDES, RC5, IDEA, dan AES dan untuk algoritma asimetrik digunakan RSA dan Elgamal. Sedangkan untuk *hash function* menggunakan SHA1 sebagai masukan untuk *Digital Signature Algorithm.* Analisa subsistem *security* dilakukan berdasarkan beberapa parameter waktu proses, distribusi frekuensi kemunculan karakter, variansi distribusi, *avallanche effect*, dan waktu untuk melakukan *brute force attack.*

Hasil penelitian ini menunjukan bahwa performasi yang paling optimal dicapai oleh AES untuk algoritma kunci simetrik dan RSA untuk algoritma kunci asimetrik untuk variansi dan *brute forced attack*-nya. Sedangkan Elgamal memilki keunggulan dalam waktu proses enkripsinya yang relatif cepat dibandingkan dengan RSA.

Kata kunci: *hybrid cryptosystem, digital signature, hash function.*