Abstrak

Surat elektronik atau yang lebih dikenal dengan email, telah menjadi sebuah media komunikasi yang sangat umum digunakan sekarang ini. Sebagian besar orang tentu sudah mengerti dan menggunakan fasilitas ini, namun tidak semua orang sadar dengan bahaya yang ada. Sebuah email sangat rentan terhadap kejahatan dunia maya (*cyber crime)* seperti contohnya penyadapan, pengubahan isi email sampai dengan pemalsuan email. Seorang ahli kriptografi bernama Phil R Zimmermann berupaya untuk memecahkan masalah keamanan email ini dengan mengembangkan sebuah teknologi kriptografi hibrida yang disebutnya PGP *(Pretty Good Privasi).* Pasangan algoritma kriptografi yang sering digunakan untuk mengenkripsi pesan dengan menggunakan PGP adalah algoritma CAST dan DH/ElGamal. Algoritma CAST dan DH/ElGamal menjadi algoritma default PGP pada beberapa versinya.

Pada tugas akhir ini akan dibangun sistem kriptografi hibrida untuk keamanan email menggunakan algoritma AES sebagai pengganti CAST dan HE-RSA sebagai pengganti DH/ElGamal. Di samping itu, untuk email yang membutuhkan pengiriman data secara aman maka diperlukannya proses pengecekan integritas dan verifikasi data sehingga dalam tugas akhir ini juga menerapkan tanda tangan digital dengan fungsi hash SHA3 sebagai masukannya. Analisis performansi dilakukan menggunakan parameter waktu proses enkripsi dan dekripsi, nilai *avalanche effect*, dan *bruteforce attack*.

Hasil dari penelitian diperoleh bahwa nilai rata-rata waktu proses enkripsi dan dekripsi kriptografi hibrida AES dan HE-RSA lebih rendah dibandingkan kriptografi hibrida CAST dan DH/ElGamal. Hasil nilai rata-rata *avalanche effect* algoritma AES-128 untuk pengujian beda *plaintext* adalah 50.9%, lebih tinggi dibandingkan algoritma CAST-128 dengan nilai 49.4%. Dan untuk nilai rata-rata *avalanche effect* algoritma AES-128 untuk pengujian beda kunci adalah 51.8%, lebih tinggi dibandingkan algoritma CAST-128 dengan nilai 47.3%. Waktu *bruteforce attack* untuk algoritma HE-RSA 1024 adalah $5.70x10^{294}$ tahun, lebih lama dibandingkan *bruteforce attack* algoritma DH/ElGamal dengan waktu $2.85x10^{294}$ tahun.

Kata Kunci: kemanan email, enkripsi, kriptografi hibrida, PGP, AES, HE-RSA.