1. Pendahuluan

1.1 Latar Belakang

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. Salah satu cara untuk memberikan keamanan email adalah dengan mengenkripsi pesan yang terdapat dalam 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 Privacy).* PGP menjadi pilihan yang populer untuk keamanan email dikarenakan kehandalan PGP sudah teruji di belahan dunia.

Tingkat keamanan pada enkripsi dengan PGP bergantung pada asumsi bahwa algoritma yang digunakan hingga saat ini belum dapat dipecahkan dengan cara kriptanalisis secara langsung dengan teknik dan peralatan yang ada saat ini[19]. Pasangan algoritma kriptografi yang banyak 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. Namun yang kita ketahui kecanggihan teknologi perangkat komputer dan perkembangan pengetahuan dalam melakukan kriptanalisis semakin membuka lebar kemungkinan ditemukannya celah keamanan kriptografi. Sehingga diperlukan suatu upaya pencegahan dengan terus melakukan penelitian untuk menemukan algoritma yang lebih baik dalam hal keamanan maupun kecepatan pemrosesannya.

Algoritma CAST yang digunakan pada PGP merupakan salah satu jenis algoritma simetrik yang cepat. Algoritma AES yang sama-sama dari jenis simetrik juga dikenal akan kemampuan kecepatannya, sehingga algoritma ini dapat digunakan sebagai alternatif CAST pada sistem kriptografi hibrida. Sedangkan algoritma HE-RSA dari jenis asimetrik merupakan varian baru hasil pengembangan dari algoritma RSA yang memberikan peningkatan keamanan dibandingkan RSA asli. Algoritma ini dapat digunakan sebagai pilihan algoritma kunci publik yang aman sebagai alternatif DH/ElGamal.

Pada tugas akhir ini akan dibangun sistem kriptografi hibrida untuk keamanan email menggunakan algoritma AES dan HE-RSA. 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. Hasil yang didapatkan dari pengujian akan dibandingkan dengan hasil pengujian algoritma *hybrid* CAST dan DH/ElGamal berdasarkan parameter waktu proses, nilai *avalanche effect* dan *bruteforce attack.*

1.2 Perumusan Masalah

Dari latar belakang masalah yang telah dijabarkan sebelumnya maka dapat di buat menjadi rumusan dan batasan permasalahan yang akan diteliti pada tugas akhir ini.

1.2.1 Perumusan Masalah

Rumusan masalah pada tugas akhir ini adalah sebagai berikut:

1. Bagaimana membangun sistem kriptografi hirbida yang lebih optimal dan memenuhi aspek *confidentiality*, *integrity*, dan *authentication* pada email?
2. Apakah performansi kriptografi hibrida AES dan HE-RSA lebih lebih baik dibandingkan *hybrid* CAST dan DH berdasarkan parameter waktu proses, nilai *avalanche effect*, dan *bruteforce attack*?

1.2.1 Batasan Masalah

Permasalah yang akan di bahas pada tugas akhir ini memiliki batasan-batasan berikut:

1. Mekanisme kriptografi *hybrid* ini menggunakan algoritma simetrik AES-128 dan algoritma asimetrik HE-RSA 1024.
2. Informasi yang akan dienkripsi dan dekripsi adalah isi pesan email dalam bentuk teks.
3. Tidak membahas pertukaran kunci publik.
4. Simulasi dilakukan dengan menggunakan bahasa pemrograman java dan mail server terintegrasi menggunakan hMailServer.

1.3 Tujuan

Tujuan yang ingin dicapai dalam pembuatan Tugas Akhir ini antara lain:

1. Merancang sistem kriptografi hibrida dengan menerapkan algoritma AES dan HE-RSA yang memenuhi aspek *confidentiality*, *integrity*, dan *authentication* pada email.
2. Menganalisa performansi algoritma *hybrid* AES dan HE-RSA serta melakukan perbandingan dengan *hybrid* CAST dan DH/ElGamal dengan parameter waktu proses, nilai *avalanche effect*, dan *bruteforce attack*.

1.4 Hipotesa

Solusi terhadap masalah keamanan email dari ancaman *cyber crime* dapat diatasi dengan melakukan enkripsi pada isi pesan email tersebut. Penggunaan PGP sebagai salah satu alat enkripsi email yang populer diasumsikan masih belum cukup aman dan cepat untuk saat ini.

Untuk mendapatkan kriptografi hibrida yang aman dan cepat maka algoritma yang akan digunakan pada skenario ini merupakan kombinasi algoritma simetrik yang terbukti memiliki kelebihan dalam hal kecepatan pemrosesan dan algoritma asimetrik yang terbukti memiliki tingkat keamanan yang lebih baik.

Berdasarkan hasil benchmark perbandingan kecepatan algoritma kriptografi[17] dan penelitian tentang perbandingan algoritma kriptografi simetrik yang melibatkan CAST, ditemukan bahwa AES lebih cepat dibandingkan CAST[18]. Sedangkan performa hasil pengujian HE-RSA berhasil menujukan peningkatan keamanan dibandingkan RSA biasa[5].

Enkripsi hibrida kombinasi algoritma AES dan HE-RSA diharapakan akan memberikan peningkatan keamanan dan waktu proses apabila dibandingkan dengan algoritma hybrid CAST dan DH/ElGamal. Penerapan metode enkripsi dan dekripsi dengan mekanisme hybrid AES dan HE-RSA ini dapat menjamin kerahasiaan dan kamanan isi pesan email sehingga dapat terhindar dari kejahatan dunia maya.

1.5 Metodologi Penyelesaian Masalah

Metodologi penyelesaian malasah dalam tugas akhir ini adalah:

a. Studi Literatur
   - Referensi dan pendalaman materi tentang *hybrid cryptosystem.*
   - Referensi dan pendalaman materi tentang berbagai algoritma kriptografi simetrik dan asimetrik.
   - Referensi dan pendalaman materi tentang AES dan HE-RSA yang akan digunakan pada tugas akhir ini.

b. Desain Sistem:
   1) Merancang desain *hybrid cryptosystem* dengan kombinasi antara algoritma kunci privat dan algoritma kunci publik.
   2) Merancang perangkat lunak yang akan mengimplementasikan kriptografi *hybrid* ini.

c. Impelementasi dan Pengujian
   Membangun sistem berdasarakan rancangan yang telah dilakukan sebelumnya dan melakukan pengujian waktu proses enkripsi, waktu proses deskripsi, nilai *avalanche effect*, dan *bruteforce attack.*

d. Analisis Hasil
   Analisis dilakukan terhadap hasil yang diperoleh dari pengujian yang telah dilakukan.

e. Penyusunan Laporan
   Pada tahap ini akan dilakukan penyusunan laporan hasil penelitian yang telah dilakukan serta membuat kesimpulan dari hasil penelitian tersebut.

1.6 Jadwal Kegiatan

Rancangan jadwal kegiatan dalam penyelesaian tugas akhir ini adalah:

Tabel 1.1 Rancangan Jadwal Kegiatan

Kegiatan	Bulan ke-1	Bulan ke-2	Bulan ke-3	Bulan ke-4
Studi Literatur				
Desain Sistem				
Testing				
Analisis hasil				
Pembuatan laporan				