# IMPLEMENTASI PROTOKOL DIFFIE–HELLMAN DAN ALGORITMA KRIPTOGRAFI RIVEST CODE 5 UNTUK ENKRIPSI DAN DEKRIPSI DALAM PENGAMANAN FILE PADA ELECTRONIC MAIL

## ABSTRAK

*Electronic mail* (*e-mail*) adalah salah satu media komunikasi digital yang popular dikalangan masyarakat saat ini. Pengaksesan media komunikasi *e-mail* mudah didapatkan oleh pengguna, menimbulkan suatu masalah baru yang membawa dampak bagi keamanan file atau data serta informasi yang sifatnya rahasia dan terbatas, sehingga informasi menjadi sangat rentan untuk diketahui serta disalahgunakan dan dimanipulasi seperti mencuri data dan mengubah isinya oleh pihak ketiga yang mencoba untuk mendapatkan informasi tersebut secara illegal. Dengan demikian dibutuhkan suatu cara untuk mengatasi permasalahan tersebut dengan menggunakan metode kriptografi. Pada penelitian ini, dibangun sebuah aplikasi pengamanan file dengan menggunakan bahasa pemograman *Borland Delphi* 7.0, *Microsoft Outlook* dan *Registry Editor* sebagai tempat penyimpanan kunci serta di dalamnya diimplementasi Protokol *Diffie-Hellman* yang fungsinya untuk melakukan pembentukan dan pertukaran kunci sesi (*session key)* yang telah disetujui antara pengirim dan penerima file juga algoritma kunci simetrik yaitu algoritma *Rivest Code* 5 untuk melakukan enkripsi dan dekripsi pada *attachment* (lampiran) file. Hasil penelitian menunjukkan bahwa Protokol *Diffie-Hellman* dan Algoritma *Rivest Code* 5 dapat dikombinasikan dengan baik, yang ditunjukkan pada pengujian enkripsi dan dekripsi, pertukaran kunci antara pengirim dan penerima file, sehingga memberikan pengamanan terhadap data. Berdasarkan hasil pengujian file sebelum enkripsi adalah D0 CF 11 E0 A1 B1 1A E1, sedangkan setelah dilakukan enkripsi hasilnya 8D 4D 35 98 F3 FF 3C B6, kemudian dilakukan dekripsi sehingga bentuk filenya berubah dan kembali dalam bentuk file awal yaitu D0 CF 11 E0 A1 B1 1A E1. Sistem keamanan file ini memiliki tingkat keamanan data yang baik serta tidak membutuhkan media penyimpanan yang besar untuk menyimpan file hasil enkripsi dan dekripsi.

*Kata Kunci: E-mail, Kriptografi, Rivest Code 5, Diffie-Hellman, Session Key.*