

INTISARI

Surat menyurat adalah salah satu metode untuk berkomunikasi antara individu, kelompok atau organisasi maupun instansi dalam desa, kota, provinsi bahkan negara. Dengan berkembangnya teknologi, surat yang dulunya dikirimkan melalui jasa pengiriman seketika berubah dengan munculnya electronic mail atau biasa disebut e-mail yang proses pengirimannya melalui media elektornik. Namun kenyataannya kenyamanan bertolak belakang dengan keamanan, pembajakan dan penipuan e-mailpun merajalela. Penulis mengusulkan aplikasi e-mail client yang menerapkan algoritma ElGamal, diharapkan hasil akhir dari aplikasi yang dibangun ini dapat bermanfaat bagi para pengguna yang menginginkan surat elektroniknya terjamin. Metode yang digunakan pada penelitian ini adalah Research and Development, metode untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Hasil penelitian ini berupa proses pembentukan kunci yang terdiri dari kunci publik dan rahasia, proses enkripsi, dan proses dekripsi.

Kata Kunci : *E-mail, ElGamal, Enkripsi, Dekripsi, Research and Development*

ABSTRACT

Mailing is one of communication methods among individual, group, or organization in the scope of village, city, province, or even country. Along with the development of technology, mailing has been using not only postal service but also electronic mail or e-mail through electronic media. However, there are consequences along with the comfort it offers, such as security issues, piracy, and online scams. This study suggests a client e-mail application that implements ElGamal algorithm to ensure the e-mail privacy. This is a Research and Development study in obtaining a certain product as well as evaluating its effectiveness. The results of this study are the process of forming the public and private keys, encryption process, and decryption process.

Keywords: *E-mail, ElGamal, Encryption, Decryption, Research and Development*