

ABSTRAK

Fajar Sukma. 53414886.

APLIKASI KRIPTOGRAFI DENGAN ALGORITMA HIBRIDA AES DAN ELGAMAL PADA FILE DIGITAL MENGGUNAKAN PYTHON

Penulisan Ilmiah, Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Gunadarma, 2017.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, *Advance Encryption Standard* (AES), ElGamal, Python.

(xv + 95 + Lampiran)

Perkembangan teknologi menyebabkan maraknya pencurian data dan penggunaan data oleh pihak yang tidak bertanggung jawab seperti *hacker*, dan *cracker*. Kriptografi dapat digunakan untuk menanggulangi permasalahan tersebut. Pada penulisan ini dibuat aplikasi kriptografi berbasis *desktop* dengan algoritma kriptografi yang digunakan yaitu algoritma hibrida *Advanced Encryption Standard* (AES) dan ElGamal yang dibuat menggunakan bahasa pemrograman python dapat digunakan untuk melakukan enkripsi dan dekripsi data untuk pengamanan. Algoritma kriptografi hibrida dipilih untuk diimplementasikan pada aplikasi karena algoritma hibrida merupakan algoritma dengan pengamanan berganda, yaitu menggunakan 2 algoritma kriptografi AES dan ElGamal sehingga membuat data atau informasi sangat sulit untuk diterjemahkan. Aplikasi dapat menerapkan cara kerja algoritma hibrida, dan aplikasi dapat melakukan proses enkripsi dan dekripsi data digital untuk mengamankan data tersebut dari pihak yang tidak bertanggung jawab, aplikasi memiliki kinerja yang baik dan juga tampilan yang sederhana sehingga membuat aplikasi mudah untuk digunakan.

Daftar Pustaka (2004 – 2017)