

ABSTRAKSI

Seiring dengan perkembangan zaman, kebutuhan manusia meningkat termasuk kebutuhan akan informasi. Kriptografi merupakan dasar untuk memahami keamanan pada komputer. Kriptografi sudah digunakan hampir di segala bidang yang terkait dengan penggunaan komputer. Begitu pentingnya kriptografi untuk keamanan informasi (*information security*), sehingga semua yang berkaitan dengan penggunaan komputer, maka orang tidak bisa memisahkannya dengan kriptografi. Kriptografi bertujuan agar pesan atau dokumen tidak dibaca oleh pihak yang tidak berhak. Pesan yang belum mengalami penyandian dikenal dengan istilah *plaintext*, dan setelah disamakan dengan suatu cara penyandian, maka *plaintext* ini akan berubah menjadi *ciphertext*. Sistem keamanan data untuk melindungi pesan, salah satu diantaranya adalah kriptografi dengan menggunakan algoritma AES. Pertimbangan bahwa sebuah standard algoritma yang baru sangatlah diperlukan untuk tetap menjaga kerahasiaan suatu data. Dalam hal ini, kunci yang lebih panjang juga merupakan keharusan.

Pembuatan aplikasi enkripsi ini menggunakan bahasa pemrograman Java, khususnya Java2 *Standart Edition* (J2SE). Aplikasi ini menggunakan algoritma kriptografi AES. Saat ini, AES digunakan sebagai standar algoritma kriptografi yang terbaru. algoritma sebelumnya dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma *Rijndael* yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit.

Kata Kunci : *AES, enkripsi, dekripsi, Java, Algoritma, kriptografi, kerahasiaan data, pembuatan, ciphertext, plaintext..*