ABSTRAK

Data dan informasi menjadi satu hal yang tidak dapat dipisahkan dari setiap aspek kehidupan manusia. Perkembangan IT (Information Technology) yang semakin cepat juga memberikan tantangan terhadap masalah keamanan data, informasi dan penyimpanannya. Kriptografi dapat menjaga agar data atau informasi tetap aman, tanpa gangguan dari pihak ketiga. Pada kriptografi terdapat banyak algoritma yang telah berkembang, diantaranya adalah algoritma AES dan DES. Akan tetapi tiap-tiap algoritma memiliki perbedaan dalam tingkat kerumitan dan proses perhitungannya. Pada skripsi ini dilakukan pengukuran dan perbandingan performasi algoritma AES (Advance Encryption Standar) dengan ukuran kunci yang fleksibel sebesar 128, 192, 256 bit dan DES (Data Encriyption Standard) denganu kuran blok 64 bit dan ukuran kunci 56 bit. Dengan menerapkan algoritma tersebut pada aplikasi berbasis Java. Kemudian dilakukan pengujian mengunakan indicator kecepatan enkripsi dan dekripsi, ukuran chipper text dan kompleksitas algoritma untuk memperoleh algoritma yang lebih unggul. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibacamanusia (plainteks) kebentuklain yang tidak dapat di megerti/dibaca oleh manusia (cipherteks). Proses transformasi plain teks menjadi cipher teks diistilahkan dengan enkripsi, sedangkan proses pengembalian pesan chipper teks menjadi plainteks diistilahkan dengan dekripsi.

Kata Kunci: *Plainteks, Chiperteks, Kriptografi, Enkripsi, Dekripsi, Data Enkryption Standard (DES), Advance Encryption Standard (AES), Android.*

ABSTRACT

Data and information become one thing that can not be separated from every aspect of human life. The rapid development of IT (Information Technology) also poses challenges to data security, information and storage issues. Cryptography can keep data or information secure, without interference from third parties. In cryptography there are many algorithms that have developed, including the AES and DES algorithms. However, each algorithm has a difference in complexity and the process of calculation. In this thesis, measurement and comparison of AES (Advance Encryption Standard) algorithm are performed with flexible key size of 128, 192, 256 bit and DES (Data Encryption Standard) with 64 bit block and 56 bit key size. By implementing these algorithms in Java based applications. Then tested using the indicator speed of encryption and decryption, chipper text size and algorithm complexity to obtain a more superior algorithm. The way it works is by changing the original / understandable message of humanity (plaintext) of other forms that can not be understood / read by humans (cipherteks). The process of plain text transformation into a text cipher is termed encryption, while the process of returning the message of the text cipher into plaintext is termed by decryption.

Keywords*: Plaintext, Chipertext, Cryptography, Encryption, Decryption, Data Enkryption Standard (DES), Advance Encryption Standard (AES), Android.*