ABSTRAK

ANALISIS APLIKASI ENKRIPSI DAN DEKRIPSI DENGAN METODE DES (DATA ENCRYPTION STANDARD)

Aris Susanto
208700771

Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan kemajuan teknologi informasi namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia harus benar-benar diperhatikan. Untuk mengatasi masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simteris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (*cipher*) yang digunakan adalah DES. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit palinteks menjadi 64 bit chiperteks dengan menggunakan 56 bit kunci internal (*internal key*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit. Algoritma dasarnya adalah pertama-tama dengan mempermutasikan dengan matriks permutasi awal (*initial permutation*), kemudian men*chiper*kannya dengan sebuah fungsi F sebanyak 16 putaran, dan terakhir adalah dengan mempermutasikannya lagi dengan invers dari matriks yang dipakai sebelumnya (*invers initial permutation*).

Kata Kunci : Kriptografi, Simetris, dan DES.

ABSTRACT

ANALYSIS APPLICATIONS ENCRYPTION AND DECRYPTION METHOD DES (DATA ENCRYPTION STANDARD)

Aris Susanto
208700771

System security of data and data's secret represent one of important aspect in growth of information technology's progress but which enough regrettably is imbalance between every growth of a technology which is not accompanied with the growth of security's system. So that a lot of system which still be weak and have to be improved by security. Therefore data security which in character secret shall really paid to attention, to overcome the problem is hence needed an application of data security which can prevent and pacify the data which we own from other people who have not business to access it. One of them is method of algorithm of cryptography symmetric, because this algorithm use the same key at the conducting process of encryption and decryption, so that our data difficult to be understood and very quickly for the encryption data. Algorithm cryptography (cipher) used is DES. DES operates on 64-bit block size. DES encrypts 64 bit plaintext into cipher text using a 64 bit key 56 bit internal (internal key). Internal lock keys raise from external (external key) 64 bits in length. The algorithm is essentially the first by permutations with initial permutation matrix (initial permutation), then the cipher with a function F as many 16 rounds, and the last is the inverse of the permutation matrix again with the previously used (inverse initial permutation).

Keywords: Cryptography, Symmetric, and DES.