TUGAS 1
DATA ENCRYPTION STANDARD & COUNTER

Kelas : KIJ - F
Kelompok F07 :
- Lucha Kamala Putri (5114100062)
- Irfan Hanif (5114100177)

PENDAHULUAN

/Pada suatu sistem jaringan, arus komunikasi data dan keamanan informasi sistem jaringan merupakan hal yang pokok yang harus dijaga. Perlu disadari bahwa untuk mencapai keamanan jaringan yang hakiki merupakan suatu hal yang sangat sulit untuk dicapai. Namun, kita mampu untuk melakukan pencegahan agar dapat mengamankan dan mengurangi gangguan terhadap keamanan informasi pada suatu sistem jaringan.

Informasi penting pada arus komunikasi data yang dikirim antar jaringan beresiko mengalami penyadapan dan bahkan pengubahan data yang dapat dilakukan oleh orang-orang yang tidak bertanggung jawab. Oleh karena itu, keamanan informasi pada arus data yang terdapat pada suatu jaringan merupakan hal yang penting untuk dilakukan./

Terdapat banyak algoritma yang digunakan sebagai metode pengamanan informasi jaringan, salah satunya adalah algoritma Data Encryption Standard (DES) dengan menggunakan mode operasi Counter (CTR).

DASAR TEORI

Data Encryption Standard

Pada bidang kriptografi, Data Encryption Standard (DES) adalah algoritma enkripsi suatu blok sandi kunci simetrik dengan ukuran blok 64-bit dan menggunakan kunci yang berukuran 56-bit.//

Counter

Counter (CTR) merupakan salah satu mode operasi yang digunakan untuk mengubah cipher blok menjadi chiper stream. Mode operasi ini membangkitkan blok keystream selanjutnya dengan mengenkripsi nilai berkelanjutan dari suatu counter. Counter tersebut dapat berupa fungsi apapun yang mengeluarkan suatu sekuens yang menjamin tidak akan berulang dalam jangka waktu panjang. Meskipun demikian, jenis counter biasa (1, 2, 3, … dan seterusnya) lebih mudah dan sering digunakan. Mode Counter (CTR) sangat cocok untuk dioperasikan pada komputer multi-processor, dimana blok dapat diekripsikan secara pararel.

LANGKAH PENGERJAAN

Berikut ini merupakan langkah pengerjaan algoritma Data Encryption Standard (DES) dengan menggunakan mode operasi Counter (CTR):
1.

KESIMPULAN

SARAN