ANALISIS DAN PERANCANGAN APLIKASI KRIPTOGRAFI KERAHASIAAN DATA MENGGUNAKAN ALGORITMA *SAFER*

NPM : 1031092
Zainal Arifin

INTISARI

SAFER (Secure and Fast Encryption Routine) adalah sebuah algoritma *block cipher* yang menjadi salah satu nominasi *AES (Advanced Encryption Standard).* Algoritma ini menggunakan kunci sepanjang *64 bit* dan panjang *block 64 bit* juga. Algoritma ini menerapkan proses enkripsi berkali-kali, normalnya sebuah teks akan mengalami perputaran enkripsi sebanyak enam ronde dan tiap ronde akan menggunakan kunci berbeda yang dibangkitkan dari kunci eksternal. Algoritma ini hanya menggunakan fungsi pergeseran, *xor*, penambahan dan pengurangan *bit* dan fungsi matematika untuk memetakan *bit*, tanpa melibatkan jaringan *feistel.* Namun algoritma ini sudah dapat memenuhi prinsip desain *confussion* dan *diffusion.*

Pada algoritma ini terdapat transformasi *linear* yang tidak lazim *(unorthodox linear transform)* yang disebut dengan *Pseudo-Hadamard Transform (PHT).* Selain itu, pada proses pembuatan kunci pada tiap ronde digunakan sebuah fungsi yang dapat menyebabkan kunci pada tiap ronde tidak menghasilkan kunci lemah *(weak key).*

Kelemahan algoritma *SAFER* adalah dalam pendistribusian kunci serta membuat jadwal kuncinya. Terutama saat menghadapi serangan *Related-Key Choosen Plaintext Attack*. Selanjutnya, laporan ini akan membahas improvisasi yang dapat dilakukan untuk memperbaiki keamanan dari algoritma ini.

Kata kunci : *Safer K-64, Advanced Encryption Standard*, enkripsi, dekripsi, keamanan.