ABSTRAK

IMPLEMENTASI ALGORITMA KRIPTOGRAFI SALSA20 UNTUK MENGAMANKAN BERKAS DOKUMEN PADA FTP SERVER

Oleh

M. Fikri Aqsha Zulfa Ismail

19102136

File Transfer Protocol (FTP) merupakan sebuah protokol jaringan untuk pengiriman berkas antar komputer. FTP diciptakan dengan tujuan untuk melakukan transmisi berkas pada jaringan komunikasi digital dengan memperhatikan aspek kemudahan, kecepatan dan efisiensi. Namun demikian, ada salah satu faktor yang penting untuk diperhatikan yaitu keamanan berkas yang dikirimkan ke dan tersimpan di FTP server. Penelitian ini menerapkan algoritma kriptografi Salsa20 untuk mengamankan data yang dikirimkan ke dan disimpan di FTP *server* dengan merancang sebuah program, salsa20 dipilih karena pada beberapa kasus lebih cepat dibanding algoritma lain seperti AES, Blowfish, ChaCha, dan RSA untuk mengenrkipsi berkas dan sampai saat ini belum ada yang mampu memecahkan *round* 20 algoritma Salsa. Hasil penelitian menunjukkan perancangan program dengan mengimplementasikan algoritma Salsa20 untuk mengenkripsi berkas berhasil dilakukan, uji fungsionalitas program berhasil berjalan sesuai dengan apa yang diharapkan, hasil menunjukkan rata – rata untuk waktu proses enkripsi 15.0 *ms* dan 14.39 *ms*, dekripsi 14.3 *ms* dan 22.4 *ms*, *download* 3890.7 *ms* dan 4120.3 *ms*, *upload* 4796.6 *m*, dan 3532.5 *ms*, pengujian *sniffing attack* menunjukkan *cipher* Salsa20 berhasil mengamankan berkas dokumen, pengujian *known-plaintext* untuk mencegah terjadi kesalahan implementasi dilakukan pembangkitan *nonce* unik pada setiap enkripsi, perhitungan *avalanche effect* menunjukkan presentase yang memenuhi kriteria SAC sehingga Salsa20 dapat dikategorikan sebagai cipher kuat.

Kata kunci: ***Algoritma Kunci-simetri, Cipher alir, File Transfer Protocol, Kriptografi, Keamanan data, Salsa20***