ABSTRACT

This paper focuses on the comparison MMB and IDEA cryptographic algorithm. MMB (Modular Multiplication-based Block cipher) using 128-bit plaintext and iterative algorithm consisting of linear steps (such as XOR and key applications) as well as the parallel application of the four major non-linear substitution which can be reversed. This substitution is determined by a multiplication modulo $2^{32} - 1$ with a constant factor, which has a higher security level than the class method. MMB using 32 bit subblock text (x_0, x_1, x_2, x_3) and a 32 bit key subblock (k_0, k_1, k_2, k_3). This makes it very suitable algorithm is implemented on a 32 bit processor. A non-linear function, f, applied six times along with the XOR function. While IDEA (International Data Encryption Algorithm) is a block cipher (cipher block), which operates on 64-bit plaintext blocks. The key length of 128 bits. The same algorithm is used for encryption and decryption. As with the other encryption algorithms, IDEA uses confusion and diffusion. IDEA algorithm uses multiplication modulo $2^{16} + 1$ operation replaces the box-S or S-Box. From the results of this comparison are discussed the differences of the two algorithms, similarity, and the superiority of the algorithm.

Keywords: MMB,IDEA, Block cipher, modulo , confusion, diffusion

ABSTRAK

Skripsi ini membahas tentang hasil aplikasi sistem enkripsi dan deskripsi data dengan metode RC5 yang nantinya memberikan kemudahan mengenai pengamanan data karena aplikasi ini tidak membutuhkan kapasitas harddisk yang besar. Agar sistem enkripsi data ini dapat berjalan dengan sempurna, pertama sekali harus ada file yang ingin di enkripsikan dan deskripsi, data yang ingin dilakukan pengamanan seperti data dalam notepad atau microsoft office. Jumlah putaran ini disimbolkan dengan r yang merupakan parameter untuk rotasi dengan nilai 0, 1, 2, sampai dengan 255. Jumlah word dalam bit disimbolkan dengan w. Nilai bit yang di support adalah 16 bit, 32 bit, dan 64 bit. Kata kunci (key word) Variable ini disimbolkan dengan b dengan range 0, 1, 2, sampai dengan 255. Key word ini dikembangkan menjadi array S yang digunakan sebagai key pada proses untuk enkripsi dan dekripsi. Data yang telah dienkripsi dikembangkan kembali menjadi 2 bagian dan disimpan di dua register A dan register B. Kemudian dilakukan rotasi ke kanan sejumlah r. Selanjutnya dilakukan operasi EX-OR yang ditandai dengan ``ă``. Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key word yang ditunjukan dengan tanda ``-``, untuk mendapatkan plaintext.

Kata Kunci: RC5, Plaintext, Word, bit , Register, Key , Enkripsi, Deskripsi