ABSTRACT

This thesis discusses the comparative study of cryptographic algorithm RSA and MD5. Message Digest 5 (MD5) key operates on 128-bit condition, divided into four 32-bit word, namely A, B, C, and D. Register A, B, C and D are initialized with hexadecimal numbers, to present the original message more of 264 bits then only 64 lower order bits are inserted. Lower order word length of the original message to be included before the high order word, the length of the result is a multiple of 512 bits. Or if in a word, the length will be equal to a multiple of 16 or 32-bit word, while RSA algorithm taking messages of less than 264 bits in length and produces a 160-bit message digest. The addition of the value of the original message length. Messages that have been given a further padding bits plus a 64 bit long message stating the original. After coupled with 64 bits long, the message will be a multiple of 512 bits. Then initialization buffer (buffer) MD. RSA algorithm in its operation requires five buffers, each the size of 32 bits so will the end result will be 160 bits. The fifth buffer in this RSA operation serves to store the results of inter-round at once to save the final result. The fifth buffer has named A, B, C, D, and E. buffers must be initialized with the values of the constants in hexadecimal notation.

Keywords: MD5, RSA, Word, bits, buffer, Lower, High

ABSTRAK

Skripsi ini membahas tentang studi perbandingan Algoritma kriptografi RSA dan MD5. Message Digest 5 (MD5) yang utama beroperasi pada kondisi 128-bit, dibagi menjadi empat word 32 bit, yaitu A,B,C, dan D. Register A,B,C dan D diinisialisasi dengan bilangan hexadecimal, untuk mempresentasikan pesan asli lebih dari 264 bit maka hanya 64 lower order bit yang dimasukkan. Lower order word untuk panjang pesan asli dimasukkan sebelum high order word, panjang dari hasilnya adalah kelipatan dari 512 bit. Atau jika dalam word, maka panjangnya akan sama dengan kelipatan dari 16 word atau 32-bit, sedangkan RSA adalah Algoritmanya mengambil pesan yang panjangnya kurang dari 264 bit dan menghasilkan message digest 160 bit. Penambahan nilai panjang pesan semula. Pesan yang telah diberi padding bits selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Setelah ditambah dengan 64 bit, panjang pesan akan menjadi kelipatan 512 bit. Kemudian inisialisasi penyangga (buffer) MD. Algoritma RSA dalam operasinya membutuhkan lima buah buffer yang masing-masing besarnya 32 bit sehingga nantinya hasil akhirnya akan menjadi 160 bit. Kelima buffer tersebut dalam operasi RSA ini berperan untuk menyimpan hasil antar putaran sekaligus untuk menyimpan hasil akhir. Kelima buffer tersebut memiliki nama A, B, C, D ,dan E. Buffer-buffer tersebut harus diinisialisasi dengan nilai-nilai konstanta dalam notasi heksadesimal.

Kata Kunci: MD5, RSA, Word, bit , buffer, Lower, High