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 ``□``. 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

ABSTRACT

This thesis discusses the results of the application encryption system and a description of the data with RC5 method that will provide ease of application data security because it does not require a large capacity hard drive. In order for this data encryption system can run perfectly, first of all there should be a file that you want to encrypt and descriptions, data such as data security to do in notepad or microsoft office. The number of rounds is denoted by r which is a parameter for rotation with a value of 0, 1, 2, up to 255. The number of word in bits denoted by w. Bit value in the support is 16 bits, 32 bits, and 64 bits. Keywords (key word) This variable is symbolized by b with a range of 0, 1, 2, up to 255. Key word developed into an array S is used as the key for encryption and decryption process. Developed encrypted data back into two parts and stored in two registers registers A and B. Then do the right rotation number r. Furthermore, the EX-OR operation are marked with ``Å``. The final stage of the reduction of the individual registers with the key word indicated by the sign `` -``, to obtain the plaintext.

Keywords: RC5, Plaintext, Word, bit , Register, Key , Encription, Description