ENKRIPSI DATA METODE BLOCK CIPHER MENGGUNAKAN TURBO PASCAL 7.0

Tri Prima Sembodo, Dra. Widaningrum Sug

Penulisan Ilmiah, Fakultas Ilmu Komputer, 2007

Universitas Gunadarma

http://www.gunadarma.ac.id

kata kunci : turbo pascal 7.0

Abstraksi :

Metode Block Cipher merupakan teknik enkripsi dimana seluruh karakter yang terdapat dalam sebuah file akan dibagi ke dalam sejumlah blok untuk kemudian diproses lebih lanjut menggunakan metode tertentu. Disini juga digunakan metode substitusi untuk menukar karakter asli dengan karakter pengganti menggunakan suatu perhitungan aritmetika, yang dilanjutkan dengan metode permutasi untuk mengubah urutan penempatan karakter sedemikian rupa dari posisi awalnya pada blok tersebut. Pada penulisan ilmiah ini dibuat perangkat lunak enkripsi menggunakan metode Block Cipher, Substitusi, dan Permutasi. Proses awal enkripsi akan dimulai dengan penentuan jumlah blok (B) berdasarkan total karakter (T) dengan B = T/4, yang berarti tiap blok akan diisi dengan 4 karakter. Tiap karakter akan dikonversi ke nilai ordinal atau nilai urutan kodenya pada ASCII untuk kemudian dilakukan perhitungan yang menghasilkan nilai ordinal baru. Nilai tersebut akan dikonversi kembali menjadi bentuk karakter pengganti berdasarkan kode barunya pada ASCII. Proses permutasi hanya digunakan untuk mengubah posisi karakter pengganti, misalnya ABCD menjadi CDBA. Sementara untuk blok terakhir yang berisi kurang dari 4 karakter, akan menjalani proses permutasi yang berbeda. Hasil percobaan menunjukkan bahwa semakin rumit perhitungan yang digunakan untuk tiap karakter, maka akan semakin sulit pula proses pemecahan algoritma enkripsinya. Namun hal tersebut akan berdampak pada lamanya waktu proses, terutama pada file berukuran besar yang mengandung banyak karakter. Karena tiap karakter harus menjalani serangkaian proses perhitungan yang panjang dan terpisah satu sama lain sebelum mendapatkan karakter penggantinya.