TINJAUAN AWAL OTENTIKASI DATA DENGAN MENGGUNAKAN ALGORITMATIGER SEBAGAI SALAH SATU ALTERNATIF

BUDI SISWANTO, ADANG SUHENDRA

Penulisan Ilmiah, Fakultas Ilmu Komputer, 2005

Universitas Gunadarma

http://www.gunadarma.ac.id

kata kunci : algoritma

Abstraksi :

Proses penyandian digunakan untuk melindungi kerahasiaan suatu data. Namun tidak dapat dijamin bahwa data tersebut masih asli dan valid. Untuk itu diperlukan teknik yang dapat mengetahui keotentikan atau keaslian data agar penerima yakin bahwa informasi yang dikirim asli dan sah. Pada penulisan Ilmiah ini dimaksudkan untuk megetahui logika dan proses algortima Tiger. Sehingga diharapkan dapat bermanfaat untuk diaplikasikan pada mesin sandi yang berorientasi pada data guna menjamin keotentikan data yang dikirim. Data dengan panjang tertentu bila dioperasikan pada algoritma Tiger akan menghasilkan nilai output (message digest) yang berbeda satu dengan yang lainnya. Hal ini dikarenakan perubahan sebagian atau seluruh data yang dioperasikan akan mengubah nilai message digest. Dengan memperhatikan sifat-sifat tersebut dan sifat-sifat yang ada pada algortima Tiger maka algoritma Tiger diharapkan dapat digunakan sebagai otentikasi.