IMPLEMENTASI BASIS BILANGAN 2K SEBAGAI SALAH SATU ALTERNATIFPEMECAHAN MASALAH PERHITUNGAN BILANGAN BULAT BERDIGIT BESAR PADA ALGORITMA RSA

AA IKSAN ARIPIN, ADANG S.,DR.,ING.,SSI,SKOM,MSC

Penulisan Ilmiah, Fakultas Ilmu Komputer, 2005

Universitas Gunadarma

http://www.gunadarma.ac.id

kata kunci : algoritma

Abstraksi :

Algoritma sistem sandi RSA tidak membatasi besarnya bilangan, baik teks beritanya maupun kuncinya. Kekuatan kriptografis sistem sandi RSA akan semakin bertambah dengan bertambahnya pula GF(n) yang dipakai. Namun saat diaplikasikan pada komputer akan ditemui keterbatasan penampungan bilangan pada komputer (tanpa program pengolahan bilangan yang khusus). Selain itu proses penghitungan pada algoritma sistem sandi RSA akan bertambah lama waktunya yang berbanding lurus dengan bertambahnya besar bilangan. Sehingga dibutuhkan suatu proses penghitungan dan penampungan bilangan yang dapat menjembatani antara ketidakterbatasannya bilangan masukan pada algortima sistem sandi RSA dengan keterbatasan yang dimiliki oleh komputer PC biasa. Komputer dalam mengolah datanya bekerja pada basis biner, sehingga pendekatan algoritma penghitungan yang paling baik diterapkan pada komputer adalah algortima penghitungan yang juga bekerja pada basis biner. Pada saat melakukan pemrogramanpun dijumpai keterbatasan penampungan bilangan pada komputer yang bergantung pada tipe bilangan yang digunakan. Sehingga diperlukan suatu manilpulasi penampungan bilangan sehingga bilangan-bilangan masukan dapat lebih besar daripada tipe bilangan yang ada. Pengimplementasian basis 2k pada algoritma sistem sandi RSA baik sebagai penampung maupun basis dasar penghitungan dapat menjembatani keterbatasan komputer dengan bilangan-bilangan besar yang harus diolah oleh algoritma sistem sandi RSA yang diaplikasikan pada komputer.