SIMULASI SISTEM KRIPTOGRAFI McELIECE DENGAN MENGGUNAKAN MATLAB

Oleh
Puji Angggraeni
013114015

ABSTRAK

Kriptografi pertama kali digunakan dalarn dunia militer untuk mengirimkan pesan rahasia. Sistem kriptografi yang digunakan pada masa itu adalah sistem kriptografi klasik. Pada sistem kriptografi klasik, d.ua pihak yang ingin berkomunikasi harus sating bertukar kunci rahasia. Pertukaran kunci rahasia tersebut menjadikan kunci sebagai mata rantai yang lemah dalarn keamanan sistem kriptografi klasik. Alasan tersebut mendorong munculnya sistern kriptografi kunci publik *(publik key cryptosystem),* yaitu sistem kriptografi yang menggunakan kunci yang ditentukan oleh pihak pengurai pesan *(dechiper),* tetapi tidak perlu diketahui oleh pihak yang ingin berkomunikasi den.gannya yaitu pihak pengirim pesan *(enchiper).* Kebanyakan keamanan sistem kriptografi kunci publik didasarkan pada sulitnya pemfaktoran bilangan bulat atau sulitnya menemukan bilangan logaritma diskret. MeEliece adalah orang pertama yang mempunyai ide tentang sistem kriptografi kunci publik yang keamanannya didasarkan pada koreksi galat pada kode koreksi galat pada kode. Tujuan dari penulisan ml adalah untuk mengetahui cara sistem kriptografi McEliece menjaga kerahasiaan pesan, dan membuat program simulasi sistem kriptografi McEliece dengan menggunakan MATLAB.

Sistem kriptografi McEliece didasarkan pada pemikiran yang sederhana, yaitu memilih kode khusus yang memiliki algoritma *decoding* yang efisien sehingga proses dekripsi menjadi lebih cepat. McEliece menetapkan untuk menggunakan salah satu kelas kode *petfect,* yaitu kode *hamming.* Selain mempunyai algoritma *decoding* yang efisien, kode hamming juga dapat mengoreksi semua galat berbobot satu yang tertambahkan pada kode sehingga proses penentuan kunci lebih cepat. Proses dekripsi pada sistem kriptografi McEliece didasarkan pada teori deteksi dan koreksi galat pada kode.

Sistem kriptografi McEilece menjaga kerahasiaan. pesan dengan tiga cara, yaitu dengan menyembunyikan kunci pribadi, mengalikan matriks generator *G* untuk kode hamming *C(n, k)* dengan matriks sebarang *S* yang *invertible* dan matriks permutasi F serta menambahkan vektor galat pada *plaintext x* yang akan dikirimkan. Proses-proses dalarn sistem kriptografi McEliece yang melibatkan matriks-matriks berukuran besar dapat diselesaikan dengan cepat dengan menggunakan program simulasi sistem kriptografi McEliece.