ABSTRAK

Setiap pesantren pasti memiliki banyak database walaupun dalam bentuk data excel, salah satunya adalah database santri yang menyimpan kerahasiaan data dan informasi dari santri. Pengamanan database santri dibutuhkan untuk melindungi data dan informasi santri dari pencurian database. Membuat sebuah sistem yang optimal dalam pengamanan database santri agar terhindar dari oknum-oknum yang tidak berhak mengakses dan mengolah data dan informasi. Database santri yang diolah dalam penelitian ini menggunakan algoritma ElGamal. Dalam pembentukan kriptografi ElGamal salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Sehingga, dengan memanfaatkan bilangan prima yang besar dengan pembentukan kunci yang menggunakan bilangan prima yang dibangkitkan secara otomatis oleh algoritma Fermat serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya akan lebih terjamin. Proses penyandian kriptografi ElGamal didahului pembentukan kunci, oleh penerima pesan. Dua macam pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik dapat di sebar luaskan sedang kunci privat untuk dirinya sendiri. Untuk membuat sebuah pesan rahasia pesan harus dikonversikan terlebih dahulu dalam bilangan bulat kemudian di kodekan berdasarkan kode ASCII (American Standard for Information Interchange). Kriptografi ElGamal memerlukan penghitungan yang lama dan sulit untuk menghasilkan algoritma yang benar-benar aman. Kelebihannya yang berbeda dan utama adalah kriptografi ElGamal menggunakan bilangan acak sehingga chiperteks tidak akan sama walaupun bloknya sama, sedangkan kelemahannya adalah dalam proses penghitungan yang cukup menyulitkan, karena angka-angka yang digunakan cukup besar. Hasil dari pengujian terhadap metode ini adalah terenkripsinya database santri. Algoritma ElGamal sangat membantu dalam pengamanan database santri pada Pondok Pesantren Darul Hikmah TPI Medan. Pada pengujian enkripsi isi database santri berhasil dienkripsi dan pada proses dekripsi dapat kembali menjadi plainteks.

Kata kunci: kriptografi, database, algoritma Fermat, algoritma Elgamal